



Universiteit
Leiden

The Netherlands

Wordt de homo digitalis bestuursrechtelijk beschermd?

Zwenne, G.J.; Schmidt, A.H.J.; Moerel, E.M.L.; Prins, J.E.J.;
Hildebrandt, M.; Tjong, Tjin Tai T.F.E.

Citation

Zwenne, G. J., & Schmidt, A. H. J. (2016). Wordt de homo digitalis bestuursrechtelijk beschermd? In E. M. L. Moerel, J. E. J. Prins, M. Hildebrandt, & T. T. T. F. E. Tjong (Eds.), *Handelingen Nederlandse Juristen Vereniging* (pp. 307-385). Deventer: Wolters Kluwer. Retrieved from <https://hdl.handle.net/1887/46377>

Version: Not Applicable (or Unknown)

License: [Leiden University Non-exclusive license](#)

Downloaded from: <https://hdl.handle.net/1887/46377>

Note: To cite this publication please use the final published version (if applicable).

Homo Digitalis

Preadviezen van

E.M.L. Moerel en

J.E.J. Prins

M. Hildebrandt

T.F.E Tjong Tjin Tai

G-J. Zwenne en

A.H.J. Schmidt

Ontwerp omslag: Corps Ontwerpers, Den Haag

© 2016 E.M.L. Moerel, J.E.J. Prins, M. Hildebrandt, T.F.E Tjong Tjin Tai, G-J. Zwenne, A.H.J. Schmidt

Alle rechten in deze uitgave zijn voorbehouden aan Wolters Kluwer. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van Wolters Kluwer.

Voor zover het maken van kopieën uit deze uitgave is toegestaan op grond van art. 16h t/m 16m Auteurswet jo. Besluit van 27 november 2002, Stb. 2002, 575, dient men de daarvoor wettelijk verschuldigde vergoeding te voldoen aan de Stichting Reprorecht te Hoofddorp (Postbus 3051, 2130 KB).

No part of this book may be reproduced in any form, by print, photoprint, microfilm or any other means without written permission from the publisher.

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(en) en Wolters Kluwer Nederland B.V. geen aansprakelijkheid voor eventuele fouten en onvolkomenheden, noch voor gevolgen hiervan.

ISBN 978-90-13-13743-9
NUR 820-102



Dhr. prof. mr. G-J. (Gerrit-Jan) Zwenne werd op 1 oktober 2011 benoemd tot hoogleraar recht en de informatiemaatschappij bij de afdeling eLaw@Leiden van de Universiteit Leiden en houdt zich vooral bezig met de toepassing en werking van de privacywet- en regelgeving, en met telecom- en internetrechtelijke vraagstukken. Gerrit-Jan is daarnaast advocaat bij het Amsterdamse kantoor Brinkhof. Verder is hij

onder meer voorzitter van de Nederlandse Vereniging voor IT en Recht (NVvIR), bestuurslid van de Vereniging Privacy Recht (VPR), docent in de VIRA-Grotius opleiding voor ICT-recht advocaten; redacteur en auteur van Tekst & Commentaar Telecom- en privacyrecht en redacteur Sdu Monografieën ICT-recht. Hij maakte onder meer deel uit van de externe klankboordgroep van de Tijdelijke Commissie ICT-projecten ('Cie Elias'), die onderzoek deed naar mislukte overheids-ICTprojecten (kamerstukken II 2014/15, 33 326, nr. 5)



Dhr. prof. mr. A.H.J. (Aernout) Schmidt werkt sinds 1975 bij de Leidse Faculteit der Rechtsgeleerdheid, eerst als computerprogrammeur en sinds 1985 in wetenschappelijke functies. In zijn promotie-onderzoek (1987, "Pallas ex Machina") liet hij zien waarom een dynamisch kennissysteem beter dan stati(sti)sche modellen een ministerieel beleid kan beschrijven. In september 2003 benoemd als hoogleraar Recht en

Informatica, is hij dat sinds maart 2010 onbezoldigd (emeritus). Zijn huidige aandacht gaat uit naar complexe, dynamische vraagstukken die in sociale systemen turbulentie veroorzaken, en naar de bijdragen die de rechtswetenschap (tezamen met andere disciplines) kan leveren om die turbulenties te domesticeren.

Wordt de homo digitalis bestuursrechtelijk beschermd?

Gerrit-Jan Zwenne en Aernout Schmidt¹

DEEL I. INLEIDING	309
1. De Homo Digitalis en de overheid	309
1.1 <i>Waarover gaat het?</i>	309
1.2 <i>Welk beeld past bij het begrip homo digitalis?</i>	311
1.3 <i>De homo digitalis getypeerd</i>	313
1.4 <i>Bestuursrechtelijke focus getypeerd</i>	315
Deel II. VERKENNING	315
2. De gedigitaliseerde overheid	315
2.1 <i>Inleiding</i>	315
2.2 <i>De gedigitaliseerde overheid en het sociaal contract</i>	317
3. Beschikbaarheid en bereikbaarheid	319
3.1 <i>MijnOverheid.nl, MijnToeslagen.nl, MijnBelastingdienst.nl (etc.)</i>	319
3.2 <i>Digitaal, tenzij...</i>	322
3.3 <i>Een recht op DigiD?</i>	322
3.4 <i>Wie bepaalt de selectie?</i>	326
3.5 <i>Samenvatting</i>	327
4. Informatieveiligheid en identiteitsinfrastructuur	328
4.1 <i>DigiD / eID-stelsel</i>	328
<i>Analogie tussen data- en wegverkeer</i>	329
<i>Het DigiD-drama</i>	330
4.2 <i>DDoS aanvallen en botnets</i>	334
4.3 <i>Samenvatting</i>	337

1. Universiteit Leiden (eLaw@Leiden).

5.	Overheidsgegevensgebruik	338
5.1	<i>Het gebruik van digitale gegevens binnen en door de overheid</i>	338
5.2	<i>De Kaderwet gegevensuitwisseling</i>	339
5.3	<i>Aftapdilemmas (of: de geheimhoudersgesprekkencasus)</i>	344
5.4	<i>Samenvatting</i>	346
Deel III. BESCHOUWING		347
6.	Evenwichtige informatieverhoudingen	347
6.1	<i>Op zoek naar tegenwicht</i>	347
6.2	<i>Zorgenkinderen</i>	348
	Risico's bij beschikbaarheid en bereikbaarheid	348
	Risico's met informatieveiligheid	349
	Risico's van overheidsgegevensgebruik	350
7.	Wat kunnen we ermee?	353
7.1	<i>In grote lijnen</i>	353
7.2	<i>Kritische aspecten</i>	354
7.3	<i>De app revolutie</i>	357
7.4	<i>Apps van de overheid</i>	360
7.5	<i>Waarheen?</i>	362
	Détournement de pouvoir digitale?	362
	Digitaal-materiële zorgvuldigheid?	363
7.6	<i>Een conclusie en enkele aanbevelingen</i>	364
APPENDICES		
	<i>Appendix 1. Iets over de homo digitalis (of de menselijke natuur) als voorwerp van rechtswetenschappelijke overweging</i>	366
	<i>Appendix 2. Veiligheid, vrijheid en grondrechten</i>	373
	<i>Appendix 3. Iets over de homo digitalis (of de menselijke natuur) als voorwerp van natuurwetenschap</i>	377
Geraadplaagde literatuur		381

DEEL I: INLEIDING

1 De Homo Digitalis en de overheid

1.1 Waarover gaat het?

In zijn rapport over iOverheid zet de Wetenschappelijk Raad voor het Regeringsbeleid uiteen hoe de overheid enthousiast informatietechnologie binnenhaalt voor haar complexe administratieve opdracht en de aanpak van urgente maatschappelijke uitdagingen, zoals daar zijn: terrorisme, veiligheid, mobiliteit en goede en betaalbare zorg.² In kamerstukken over de digitale overheid worden haar ambities vooral gearticuleerd in steekwoorden of slogans als ‘de verbetering in kwaliteit van digitale overheidsinformatie en overheidsdienstverlening’, ‘administratieve lastenvermindering’ en ‘regeldrukreductie’, het realiseren van ‘efficiencywinsten’ enz.³ De terminologie suggereert dat digitalisering geen of slechts een beperkte impact heeft op de rechtspositie van burgers, consumenten, werknemers, studenten, belastingbetaler, cliënten, verzekerden, automobilisten, treinreizigers, patiënten, etc. Of, sterker nog, dat deze rechtspositie vooral zou worden versterkt doordat de hen toekomende rechten met minder moeite geëffectueerd kunnen worden. Uiteenlopende voorbeelden laten zien dat die suggestie niet altijd terecht is.

De digitalisering van de overheid verandert haar verhouding ten opzichte van burgers. Het is niet zo dat de positie van de burger in alle gevallen wordt verzwakt, maar we kunnen wel een paar gevallen noemen waar er tenminste de zorg is dat daarvan sprake kan zijn. DigiD biedt een voorbeeld. DigiD is de persoonlijke inlogcode waarmee burgers zich identificeren bij de digitale overheid en die wordt gebruikt voor het aanvragen van toeslagen als de kinderopvangtoeslagen, huur- en zorgtoeslagen. Door de zgn. Bulgarenfraude, die in april 2013 aan het licht werd gebracht, is duidelijk dat er daarbij nogal eens wat mis kan gaan.⁴ Toch kunnen aanvragers van toeslagen die stellen slachtoffer te zijn van identiteitsfraude niet op veel begrip rekenen bij de bestuursrechter. Omdat de aanvraag voor de toeslag was ingediend op haar naam moest het volgens de bestuursrechter ervoor worden gehouden dat deze is gedaan met haar toestemming, dan wel dat zij haar persoonlijke en geheime DigID-code aan een ander heeft verstrekt. In de beide gevallen komt de onjuistheid van de aanvraag voor

2. WRR, iOverheid, rapport nr. 86, Den Haag / Amsterdam 2011, p. 11, 34 en 93.

3. Zie bijv. *Kamerstukken II* 2012/13, 26643, nr. 280, p. 1-2.

4. RTL Nieuws, ‘Grootschalige fraude Bulgaren met toeslagen’, 21 april 2013 www.rtl-nieuws.nl/nieuws/binnenland/grootschalige-fraude-bulgaren-met-toeslagen en daaropvolgende nieuwsberichten.

haar rekening. En daaraan doet niet af dat de toeslagen waren uitbetaald op een rekeningnummer dat niet van de aanvrager was.⁵

Deze zaak staat niet op zichzelf. Het risico van misbruik van DigiD wordt doorgaans gelegd bij de burger, ook als die niet zo digivaardig is als door de overheid wordt verondersteld.

Een ander voorbeeld van veranderende burger-overheid verhoudingen vinden we in het omvangrijke, en diep in de persoonlijke levenssfeer ingrijpende, overheidsdigitaliseringsproject dat beoogt te komen tot een integraal optreden ten aanzien van – het is een hele mond vol – de voorkoming en bestrijding van onrechtmatig gebruik van overheidsmiddelen en overheidsvoorzieningen op het terrein van de sociale zekerheid en de inkomensafhankelijke regelingen, de voorkoming en bestrijding van belasting- en premiefraude en het niet naleven van arbeidswetten. Een recente grondslag daarvoor is te vinden in het zogeheten SyRI-besluit dat beoogt fraudeaanpak mogelijk te maken door gegevensuitwisseling en het effectief gebruik van de binnen de overheid bekend zijnde gegevens. In het kader daarvan wordt voorzien in een bevoegdheid tot risicoprofilering in het Systeem Risico Indicatie of SyRI (voorheen wel aangeduid als 'black-box')⁶ dat lijkt te zijn bedoeld om *big data predictive analytics* mogelijk te maken.⁷ Ook dat kan moeilijk worden gezien als versterking van de positie van de digitale burger, al was het maar in termen van bewijspositie of onschuldpresumptie: een burger met een verdacht profiel loopt het risico zich te moeten verweren tegen digitale verdachtmakingen of 'digitale predestinatie'.⁸

In dit preadvies verdiepen wij ons in de rechtspositie van de mens, *homo digitalis*, die zich moet zien te handhaven in een gedigitaliseerde wereld en die daarin een weg moet zien te vinden. Om te beginnen zetten we in dit eerste hoofdstuk uiteen wat we bedoelen met de notie van *homo digitalis* voor de bestuurder en de bestuurd. We ontlelen daarbij inzichten aan andere menstyperingen, zoals de *homo economicus*, de *homo ludens*, *homo universalis* etc. en lichten ze toe in Appendix 1. Vervolgens doen we in de hoofdstukken 2 tot en met 5 een poging aan de hand van voorbeeldsituaties te inventariseren, te categoriseren en te analyseren met welke risico's of bedreigingen de *homo digitalis* te maken kan krijgen als gevolg van digitalisering bij de overheid. Daaraan koppelen wij welke positiefrechtelijke

5. ABRvS 28 november 2012 ECLI:NL:RVS:2012:BY4444.

6. D. Stokmans, 'Sociale Zaken overtrad mogelijk de privacywetgeving', *NRC* 3 oktober 2014

7. Besluit van 1 september 2014 tot wijziging van het Besluit SUWI in verband met regels voor fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens met inzet van SyRI, *Stb.* 2014, 320.

8. De term is van de voorzitter van onze privacytoezichthouder, Jacob Kohnstamm, in zijn speech voor het ExpertForum van de Nationale DenkTank 2014 op 3 oktober 2014 (https://cbpweb.nl/sites/default/files/atoms/files/speech_big_data_nationale_denktank_versie_3_okt_2014_website.pdf, laatst geraadpleegd op 22 december 2015)

middelen het bestuursrecht te bieden heeft om deze het hoofd te bieden, en of er daaraan iets hapert. We vatten dit ruim op. We gaan het vervolgens in hoofdstuk 6 hebben over burgers en andere bestuurden (organisaties, ondernemingen etc.) die een andere positie krijgen c.q. innemen ten opzichte van de digitaliserende c.q. gedigitaliseerde overheid. Tenslotte komen we in hoofdstuk 7 tot een slotbeschouwing, waarin we één en ander samenbrengen, en met conclusies en aanbevelingen, met daarbij aandacht voor generaliseerbaarheid, en voor wat we wel en niet kunnen verwachten van het bestuursrecht als sturingsinstrument.

Het is ondenkbaar dat we in deze bijdrage volledig kunnen zijn. In het vervolg haken we aan bij de belangrijkste punten uit de ‘visiebrief digitale overheid’ van de minister van BZK uit 2013, een brief die ook rept over de gewenste toestand in 2017. Zo zorgen we ervoor dat onze bijdrage tenminste aansluit bij de dominante politieke denkkaders van het moment. We selecteren een viertal ambities zoals die door de minister worden onderkend. We zien elk van die ambities onder ogen, op zoek naar het antwoord op de vraag hoe de homo digitalis zich zal kunnen houden onder de verwachte wijzigingen die in het kader van genoemde ambities zullen optreden. We gaan daarbij enigszins anekdotisch te werk en beperken ons tot het geven van voorbeelden uit een praktijk die ons bekend is. Aan het eind van elk van deze verkennende en inventariserende hoofdstukken vatten we de geïdentificeerde risico’s in enigszins gegeneraliseerde vorm samen, om in een later deel naar eventuele oplossingen te kunnen zoeken.

1.2 Welk beeld past bij het begrip *homo digitalis*?

Om eerlijk te zijn was het ons niet onmiddellijk helder wat met de term *homo digitalis* werd bedoeld toen ons werd gevraagd vanuit dat perspectief te redeneren.⁹ We voelden weliswaar meteen aan waarom dat begrip toepasselijk is, maar zagen ons ermee geconfronteerd dat het begrip nog niet is ingeburgerd en in het recht geen standaardinterpretatie kent. Een verkennend literatuuronderzoekje wees uit dat antropologen het begrip vooral gebruiken om menselijk gedrag te typeren zoals dat zich op het moment in het westen openbaart. Vanuit een collectivistisch perspectief wordt het begrip gebruikt bij het duiden van de sociale behoeften en mogelijkheden van individuen, zoals bij het gebruik van sociale netwerken, bijv. bij revolutionaire bewegingen). En vanuit een individualistisch georiënteerd perspectief wordt het begrip ingezet om verwachtingen met betrekking tot kunstmatige intelligentie te duiden.

In dit pre-advies brengt onduidelijkheid over het begrip *homo digitalis* ons waarschijnlijk in de problemen. Als conceptueel anker moet het begrip onmiddellijk en zonder veel voorbereiding aanspreken. We hebben daar-

9. Een nadere onderbouwing voor deze paragraaf is opgenomen in Appendix 1.

om een werkdefinitie nodig. We hakken de knoop als volgt door en geven de definitie waarvan wij in deze bijdrage uitgaan:

Een homo digitalis is een homo sapiens (mens) die zich in meer of mindere mate laat vertegenwoordigen of laat leiden door één of meer gedigitaliseerde processen, en die dus leeft en moet leven en overleven in een wereld of omgeving die dat mogelijk maakt.

We denken dat deze betekenis overeenkomt met wat intuïtief wordt begrepen door wie de term zonder nadere toelichting hoort.

Het is dan van belang dat ons begrip van *homo digitalis* een meerwaarde heeft in vergelijking met wat de verschillende andere, verwante deelbegrippen te bieden hebben voor de analyse van de menselijke natuur. We denken daarbij aan begrippen die zich inmiddels hebben gevestigd, zoals de *homo universalis* (drager van kennis, het ideaalbeeld uit de verlichting), *homo economicus* (met oog voor profijt en gezond eigenbelang), *homo ludens* (spelend van aard, innovator) en natuurlijk *homo sapiens* (het kunnen reflecteren, als biologische soort). Het is ook voor de rechtswetenschap nodig om aannamen te doen over de menselijke natuur die meebepaalt wat wel en wat niet juridisch kan zijn. Het recht gaat er van uit dat de mens als rechtssubject een vrije wil heeft, bewust keuzen kan maken en verantwoordelijkheid voor zijn handelen kan dragen, en dat de mens drager is van fundamentele rechten en vrijheden, zoals het recht op bescherming van zijn of haar persoonlijke levenssfeer.

Onze fascinatie met de *homo digitalis* wordt gevoed door het inzicht dat die mens ook juridisch moet zien te overleven in een wereld waarin de technologische mogelijkheden soms op verbijsterende wijze toenemen en veranderen. Wij houden in deze bijdrage als fundamentele van de rechtswetenschap vast aan uitgangspunten van vrije wil, bewust kiezen en verantwoordelijkheid dragen. De meerwaarde van het gebruiken van de definitie is dan, dat we daarmee duidelijk maken dat we er niet op uit zijn om naar een nieuw fundament voor het recht te zoeken waarin, bijvoorbeeld kunstmatig intelligente toepassingen ook verantwoordelijkheid dragen, maar naar mechanismen die het mogelijk maken voor respectievelijk overheden en burgers (d.w.z. bestuurders en bestuurden) om hun rol als dragers van verantwoordelijkheden te blijven spelen.

Met de *homo universalis*, de *homo sapiens*, de *homo ludens* en de *homo economicus* hebben we dus, zeker als die wordt aangevuld met de *homo digitalis*, de beschikking over een kleine familie van begrippen die bruikbaar zijn om bij het analyseren van situaties rekening te houden met essentieel geachte onderdelen van de menselijke natuur. Dat stelt ons in staat om nieuwe situaties die het recht uitdagen evenwichtig te behandelen. Zoals veel van de economische wetenschap rust op een mensbeeld van de redelijk handelende partijen vanuit goed begrepen eigenbelang, zo rust veel

van de rechtswetenschap op een mensbeeld van verantwoordelijkheid en vrije wil.¹⁰

In beleidsdocumenten en kamerstukken wordt de term ‘digitalisering’ vaak probleemloos zonder toelichting gebruikt.¹¹ Wij verstaan eronder het gebruik van moderne elektronische informatie- en communicatietechnologie om processen en procedures langs elektronische weg, en dus in digitale vorm, te laten verlopen. Het gaat bij digitalisering om de veranderingen die zich voltrekken in de maatschappij en de economie ten gevolge van deze technologie. We zien digitalisering als een groeiende kracht die de omgeving vormt voor menselijk handelen en die tegelijkertijd *zelf* het gevolg is van acties van rechtssubjecten.

Het gaat ons in deze bijdrage om verantwoorde besluitvorming, de legitimering daarvan en de rechtsbescherming in verband daarmee. In onze aanpak wordt derhalve met de term *homo digitalis* allereerst gerefereerd aan een verantwoordelijk individu, maar verder als dat zo uitkomt ook aan de individuen die deel uitmaken van instituties en instellingen, rechtspersonen, bestuursdiensten, ondernemingen en andere organisatievormen. In voorkomende gevallen zal dat met zich brengen dat we dergelijke organisatievormen in het taalgebruik in minder of meerdere mate vereenzelvigen met de desbetreffende individuen die alleen of met anderen invloed hebben op de wijze waarop deze in het maatschappelijk verkeer optreden. Een andere benadering, waarbij we het begrip rigide zouden opvatten, heeft het risico dat ons blikveld te beperkt wordt en dat we geen zicht hebben op belangrijke rechtspositionele implicaties die het gevolg zijn een toeneemende verdichting van de digitale dienstverlening en van digital organisatievormen.

We gaan dus ervan uit dat de *homo digitalis* als autonoom individu voor zich handelt, en zijn ons ervan bewust dat zijn rol lijkt te verminderen en te veranderen wanneer hij optreedt als functionaris c.q. vertegenwoordiger van bijvoorbeeld een onderneming of overheidsdienst.

1.3 *De homo digitalis getypeerd*

Onze definitie staat uiteenlopende representanten van de ‘soort’ *homo digitalis* toe. Ertoe worden gerekend bestuurders en bestuurden of burgers, waarvan de laatstgenoemden afhankelijk van feitelijke en juridische

10. Wij kiezen ervoor, om de druk die wel vanuit de neurowetenschappen op deze aanname wordt uitgeoefend (bijvoorbeeld op basis van de ‘Libet data’) onder verwijzing naar en Dennett en Kinsbourne (1992) als irrelevant naast ons neer te leggen omdat het recht – ook als het, onder verwijzing naar Fuller (1930), mede berust op een fictie – een uiterst waardevol maatschappelijk spel oplevert waarvoor wij niet onmiddellijk een nieuw fundament zien. Met andere woorden: hoe verleidelijk misschien ook, we gaan niet op zoek naar een geheel nieuwe fundering voor de rechtswetenschap.

11. Zie bijv. *Kamerstukken II* 2014/15, 34 059, nr. 3.

omstandigheden allerlei hoedanigheden kunnen hebben, zoals die van consument, student, werknemer, werkgever, verzekerde, patiënt, automobilist, treinreiziger, zzp-er of andersoortig ondernemer, kiezer, et cetera.

Als gezegd gaat het in dit preadvies om de rechtspositie van de mens, *homo digitalis*, die zich moet zien te handhaven in een gedigitaliseerde wereld en daarin zijn weg moet vinden. We gebruiken vooral de begrippen ‘bestuurder’ en ‘burger.’ Onder de laatste verstaan we ook de ‘ondernemer’¹² als iemand, die handelt in de uitoefening van een beroep of bedrijf. Voor deze ondernemers zal, in het kader van dat beroep of bedrijf, vooral betekenis toekomen aan aspecten als ondernemingsvrijheid, *level playing field* en, wie weet, ook innovatie.¹³

Het gaat ons vooral om de verhoudingen van burgers of ondernemers ten opzichte van bestuurders, en dus niet om die van burgers ten opzichte van ondernemers en omgekeerd. We beperken ons daarom tot de verhoudingen waarin de bestuurder een rol speelt. Om de typering in actie te bezien geven we een handvol soms hypothetische situaties waarbij het bijvoorbeeld gaat om de relaties tussen offline burgers en digitale bestuurders, en omgekeerd, van digitale burgers ten opzichte van offline bestuurders. De rapporten en onderzoeken van de Nationale ombudsman bieden daartoe voorbeelden. Zo is er het voorbeeld van iemand die zijn baan verliest en vervolgens niet de mogelijkheid heeft om zijn bijstandsuitkering langs digitale weg aan te vragen.¹⁴ Een omgekeerde situatie, digitale burger tegenover offline bestuurder, betreft een Wob-verzoek dat in de gemeente Delft niet in digitale vorm kon worden gedaan.¹⁵

Een opmerkelijk slecht gedocumenteerd voorbeeld – de technische analyse van Fox-IT ervan is maar ten dele openbaargemaakt¹⁶ – van de verhouding tussen digitale burgers of ondernemers tegenover offline of online bestuurders, is dat van de vermoedelijk Iraanse hackers die erin slaagden de digitale certificaten van Diginotar te vervalsen, en daarmee de bestuurders volledig verrasten.

12. Aldus sluiten we aan bij de gebruikelijk categorie-indelingen op belangrijke overheidswebsites, zoals overheid.nl en belastingdienst.nl, waar ook wordt uitgegaan van de categorieën «burgers of particulieren» en «ondernemers of bedrijven»; zie ook bijv. *Kamerstukken II* 2015/16, 26 643, nr. 373, p. 1.

13. Deze indeling sluit aan bij het onderscheid dat wordt gemaakt in het Dialogic onderzoek ter ondersteuning van de zgn. visiebrief digitale overheid 2017 van de minister van BZK 23 mei 2013, *Kamerstukken II* 2013/2014, 26 643, nr. 280. In dit onderzoek werd onderscheid gemaakt naar (1) digitaal niet-redzamen, (2) digitaal redzamen met ondersteuning, en (3) digitaal zelfredzamen. Zie Gillebaard en Vankan (2013). Zie ook Nationale ombudsman, *De burger gaat digitaal*, 2013/170, 9 december 2013, p. 13.

14. Nationale ombudsman, *De burger gaat digitaal*, 2013/170, 9 december 2013, p. 7.

15. No. Rapport 2014/113.

16. De Onderzoeksraad voor Veiligheid deed wel onderzoek, zie Onderzoeksraad voor Veiligheid (2012).

Een ander voor de verhoudingen van burgers en ondernemers tegenover digitale bestuurders interessant voorbeeld vinden we in het streven van de bewindspersoon verantwoordelijk voor veiligheid en justitie, om domein-overschrijdende fraude in beeld te brengen en te bestrijden door te komen tot ‘volledige uitwisseling van informatie,’ en op grond van deze informatie analyses te maken die een ‘integraal en effectief optreden’ mogelijk moeten maken.¹⁷

1.4 Bestuursrechtelijke focus getypeerd

Traditioneel gaat het algemene bestuursrecht uit van het legaliteitsbeginsel, hetgeen zoveel wil zeggen dat het bestuur alleen bevoegd is om dat te doen waarvoor een wettelijke basis is gelegd. Eén van de vragen die we onder ogen zullen moeten zien is wat voor de verhouding van de digitale overheid ten opzichte van de digitale burger de betekenis kan zijn van het legaliteitsbeginsel en dan in hoeverre het voor digitale bestuurders een lege huls dreigt te worden, en wat we daartegen kunnen doen.

Een andere vraag die we onder ogen moeten zien is in hoeverre het bestuur zich kan, mag of moet overgeven aan samenwerkingsverbanden met experts uit het bedrijfsleven (en, wie weet, met experts uit de wetenschap) en op welke wijze de mandaterings- en verantwoordelijkheidsbetrekkingen transparant en effectief kunnen worden, of blijven. Het is voorts ons vermoeden dat, zoals de WRR aangaf, een inventarisatie van de digitale werkelijkheid aan het licht brengt dat daarmee aan steeds meer grote en complexe problemen het hoofd moet worden geboden, zoals daar zijn extremisme en terrorisme, veiligheid, mobiliteit of goede en betaalbare zorg – problemen die alleen nog maar voldoende lijken te kunnen worden begrepen door specialisten uit diverse disciplines te laten samenwerken.¹⁸

In het volgende deel gaan we verkennen. We bekijken de bestuursrechtelijke risico's, de rechtsmiddelen en de zwaktes daarin.

Deel II. VERKENNING

2. De gedigitaliseerde overheid

2.1 Inleiding

In wat met enig gevoel voor overdrijving wordt aangeduid als een ‘visie-brief’ geeft minister Plassterk een uiteenzetting van de pijlers of ambities

17. *Kamerstukken II* 2014/15, 32761, nr. 79.

18. WRR (2011) p. 11, 34 en 93.

waarop anno 2013 het kabinetsbeleid voor de digitalisering van de overheid steunt.¹⁹ Deze pijlers bieden, ook al zijn ze misschien niet zo bedoeld, een goed vertrekpunt voor onze inventarisering van de rechtsposities van de homo digitalis, als burger en ondernemer en als bestuurder. Wij geven daaraan onze eigen draai en gebruiken deze pijlers om te komen tot een praktische indeling van aandachtsgebieden.²⁰ Aan de hand daarvan verkennen we dan op welke wijze digitalisering verschuivingen met zich brengt van de rechtsverhoudingen van de onderscheiden varianten van de homo digitalis ten opzichte van elkaar. Het gaat om de volgende aandachtsgebieden:

- de digitale beschikbaarheid van relevante overheidsinformatie en het bevorderen van de mogelijkheden tot digitale communicatie met de overheid (verkort aangeduid als ‘beschikbaarheid en bereikbaarheid’);
- het waarborgen van informatieveiligheid en in verband daarmee het realiseren van een betrouwbare identiteitsinfrastructuur (‘informatie-veiligheid en identiteitsinfrastructuur’);
- het verbeteren van het gebruik van digitale gegevens binnen en door de overheid (‘overheidsgegevensgebruik’);
- het versterken van de informatiepositie van de burger en ondernemer ten opzichte van de versterkte informatiepositie van de digitale overheid (‘evenwichtigheid van informatieverhoudingen’).

Aan de eerste drie van de hierboven genoemde aandachtsgebieden wordt in de brief expliciet aandacht besteed. Aan het vierde aandachtsgebied wordt in de brief maar beperkte aandacht gegeven, maar het lijkt ons het belangrijkste omdat het oplossingen biedt voor de problemen die in de drie voorafgaande gebieden naar boven zijn gekomen. Wij behandelen het daarom afzonderlijk in het afsluitende deel van dit pre-advies.

Voor ieder aandachtsgebied bespreken we voorbeeldsituaties die inzichtelijk maken waar de homo digitalis tegenaan loopt en waarin hij met de middelen die het bestuursrecht biedt zijn weg moet zien te vinden. Voor elk aandachtsgebied wijden we ook een korte beschouwing aan de vraag

19. In de visiebrief (*Kamerstukken II* 2012/13, 26 643, nr. 280) worden deze pijlers op de volgende wijze aangeduid: (1) informatie moet online beschikbaar zijn; (2) burgers kunnen alle (aan)vragen aan de overheid digitaal versturen en alle berichten van de overheid digitaal ontvangen; (3) gebruiksvriendelijkheid en toegankelijkheid; (4) inzage- en correctierecht voor burgers; (5) informatieveiligheid en stelsel eID; (6) optimaal gebruik van digitale gegevens door de overheid; (7) samen verder bouwen aan een gezamenlijke infrastructuur; (8) huidige financieringswijze leidt tot inefficiënte eigen oplossingen.
20. We kiezen er mede gelet op de maatschappelijke urgentie van hoe de problematiek zich ontwikkelt in deze bijdrage uitdrukkelijk voor om aansluiting te zoeken bij het politiek-juridische discours zoals dat thans gaande is in plaats bij het voornamelijk positiefrechtelijke discours (waarmee onze bijdrage natuurlijk wel samenhang vertoont) zoals mede gevoerd door Barkhuysen et. al. (2014), Franken (1993), Groothuis (2011), Groothuis (2013), Overkleeft-Verburgh (1999), Overkleeft-Verburgh (2014),.

of de voorliggende transitie van onze samenleving, van offline naar digitaal, ook systeemrisico's (d.w.z. een risico dat aan het systeem als geheel en aan het complex van deelsystemen is verbonden) met zich meebrengt, en zo ja welke, en of daartegen vormen van rechtsbescherming in de beschouwing zouden moeten of kunnen worden betrokken.²¹

2.2 *De gedigitaliseerde overheid en het sociaal contract*

Het spreekt waarschijnlijk niet helemaal vanzelf hoe deze vier aandachtsgebieden samenhangen met een meer algemeen beeld van de krachten en beginselen die een rol hebben gespeeld (en nog spelen) bij de ontwikkeling van onze rechtssystemen, en de rollen (bevoegdheden, taken, plichten) die aan het bestuur worden toegekend. In het onderwijs van de Leidse rechtenfaculteit wordt bij het vak Encyclopedie de nadruk gelegd op enkele belangrijke ontwikkelingen in het rechtsdenken over het sociaal contract. Wat ons daarbij van belang voorkomt is dat in die ontwikkeling een aantal stappen kan worden herkend die laten zien dat er een aantal centrale concepten spelen: soevereiniteit, een geweldsmonopolie, de Rule of Law, de scheiding der machten en de algemene wil van een volk.²²

In deze weg naar Westerse democratieën is de verhouding burger-soeverein weergegeven als een zich ontwikkelend concept. Die ontwikkeling verliep langs steeds betere manieren om het nodig geoordeelde geweldsmonopolie te brengen naar een bestuur dat steeds minder het risico in zich bergt van geweldsusurpatie. Ten eerste door de nadruk van bestuurstaken te leggen op het beschermen van vrijheid (vanaf Locke) in plaats van veiligheid. Ten tweede door grondrechten te formuleren (de Rule of Law) die grenzen stellen aan de wetgeving (doelbinding aan verwezenlijking van vrijheid). Ten derde door het bestuur in drie onafhankelijke instituties onder te brengen, en de wetgeving en de rechtspraak los te maken van het eigenlijke bestuur (machtscheiding). Ten vierde, tenslotte, door de grondrechten als uiting te zien van de algemene wil van een volk, waaraan het bestuur zijn gezag ontleent.

In feite, en in grove lijnen, werden de Europese staten bijna allemaal tot ver in de negentiende eeuw bestuurd door nauwelijks door wetgeving ingetoomde absolute vorsten, of hun functionele equivalenten. De ideeën rond hoe regimes te verbeteren hebben in de loop der tijd vorm gekregen en zijn de daaropvolgende periodes ook verwezenlijkt, in het bijzonder

21. Hiermee wijkt onze benadering nogal af van het ons inziens overigens waardevolle Panteia onderzoek uit 2015 naar hoe de knelpunten bij de (digitale) overheid kunnen worden voorkomen en opgelost, omdat daar in "In overleg met de opdrachtgever is afgesproken dat de focus hierbij ligt op knelpunten bij de invoer van gegevens en gegevensverwerking, waar burgers het slachtoffer van worden." (p. 15). Ons perspectief is anders.
22. Die stappen zijn functioneel weergegeven in Appendix 2.

rond de Amerikaanse onafhankelijkheid, de Franse Revolutie, het Weense Congres van 1815 en de ‘democratische lente’ van 1848. In de geschetste ontwikkeling kan in grote lijnen een accentverschuiving worden waargenomen: van het primaat van de bescherming van individuele *veiligheid* naar het primaat van de bescherming van individuele *vrijheid*.

Eén en ander betekent dat de macht van het offline bestuur van de twintigste eeuw, voorafgaand aan de opkomst van de ICT,²³ werd beperkt door de wet (legaliteitsbeginsel), dat het bestuur een onafhankelijke institutie was naast de wetgever en de rechtspraak (machtscheiding) en dat het bestuur als opdracht had om de grondrechten van individuele burgers te beschermen.²⁴

We hebben deze beschouwing aan de ontwikkeling van onze bestuursrechtelijke arrangementen naar voren gebracht omdat we menen dat de ontwikkeling van onze samenleving van offline naar digitaal een misschien onverwachte wending neemt waar het gaat over hoe het gesteld is met onze individuele veiligheid en onze individuele vrijheid. We bezien of we de vier aandachtsgebieden die we in de brief van Plasterk herkennen kunnen plaatsen in dit spanningsveld:

- de digitale beschikbaarheid van relevante overheidsinformatie en het bevorderen van de mogelijkheden tot digitale communicatie met de overheid (verkort aangeduid als ‘beschikbaarheid en bereikbaarheid’) is essentieel voor de **individuele vrijheid** van de burger; vrijheid is immers nooit absoluut en kan door overheidsbesluiten en regelingen worden ingeperkt. Beschikbaarheid en bereikbaarheid van heldere informatie daarover maakt de overblijvende, vrije ruimte kenbaar.
- Het waarborgen van informatieveiligheid en in verband daarmee het realiseren van een betrouwbare identiteitsinfrastructuur (‘informatie-veiligheid en identiteitsinfrastructuur’) is essentieel voor **individuele vrijheid en individuele veiligheid**; want de informatieveiligheid is nodig voor effectieve beschikbaarheid en de identiteitsinfrastructuur is nodig tegen de gevaren van identiteitsdiefstal - van de burger, maar ook van de overheid (DigID!).
- Het verbeteren van het gebruik van digitale gegevens binnen en door de overheid (‘overheidsgegevensgebruik’) wordt onder andere **gedaan om individuele veiligheid** zeker te stellen, maar doet vaak af aan **individuele vrijheid**; als argument voor de huidige datahonger van de overheid wordt vaak gewezen op de noodzaak om bescherming te bieden tegen ernstige misdrijven en terroristische dreigingen, maar diezelfde datahonger leidt er ook toe dat de beschikbare gegevens worden ingezet voor steeds meer (ook proactieve) vormen van handha-

23. Zie voor een analyse van de veranderende rol van de rechter in dit verband ook: Barkhuysen et al. (2014).

24. In deze geest ook al Overkleeft-Verburg (1999).

- ving door de overheid; privacy is een belangrijke voorwaarde voor individuele vrijheid, en die verzwakt op deze wijze fundamenteel.
- Het versterken van de informatiepositie van de burger en ondernemer ten opzichte van de versterkte informatiepositie van de digitale overheid ('evenwichtigheid van informatieverhoudingen') beoogt bij te dragen aan **individuele vrijheid**; immers wanneer er een verschil van inzicht bestaat tussen een burger of bedrijf met de overheid over een overheidsbesluit of regeling (of de manier waarop die wordt gehandhaafd) is het resultaat mede afhankelijk van de mate waarin de informatieposities van beide partijen in evenwicht zijn. Een zekere mate van *equality of digital arms* is noodzakelijk voor het kunnen verdedigen, tegen de overheid, van de individuele vrijheden van homo digitalis.

En inderdaad, wanneer we naar de aandachtsgebieden kijken gaat het op het eerste gezicht steeds om de individuele vrijheid en veel minder vaak over individuele veiligheid van de burger. Met deze vaststelling komen we nu toe aan het verkennen en inventariseren van de risico's die we herkennen bij de drie expliciet behandelde aandachtgebieden uit de visiebrief.

3. Beschikbaarheid en bereikbaarheid

3.1 *MijnOverheid.nl, MijnToeslagen.nl, MijnBelastingdienst.nl (etc.)*

Onder wat wij hebben aangeduid als 'de digitale beschikbaarheid van relevante overheidsinformatie' wordt in de visiebrief²⁵ begrepen het streven dat alle als relevant gekwalificeerde overheidsinformatie digitaal beschikbaar wordt gesteld.²⁶ Erbij horen de uit de Angelsaksische wereld afkomstige initiatieven als 'open overheid' en 'open data'.²⁷ Het gaat niet alleen om het verbeteren van de publieke dienstverlening, maar ook om de kwaliteit van het openbaar bestuur en in dat verband het kunnen beïnvloeden van bestuurlijke besluitvorming, de controle daarop en de evaluatie ervan. Waar het de doelstellingen betreft die verband houden met open data initiatieven, gaat het ook om het mogelijk maken dat nieuwe informatieproducten, -diensten en -toepassingen door het bedrijfsleven worden ontwikkeld,

25. *Kamerstukken II 2012/13*, 26 643, nr. 280, p. 3.

26. Bij het schrijven van dit hoofdstuk is dankbaar gebruik gemaakt van S.R. Klaassen *Elektronisch verkeer met de overheid via de Berichtenbox. Een toekomstbestendig wetmatig kader?* 1 september 2015 (ongepubliceerd).

27. *Kamerstukken II 2012/13*, 26 643, nr. 280, p. 3; zie ook bijv. het Actieplan Open overheid, van het Ministerie BZK uit september 2013; of de website open-overheid.nl waar we al op de landingspagina een citaat van Barack Obama krijgen gepresenteerd (geraadpleegd 1 augustus 2015).

waarmee economische groei wordt gestimuleerd en maatschappelijk engagement wordt bevorderd.²⁸

Verwant daaraan is de, ook in de visiebrief tot uitdrukking gebrachte ambitie dat de overheden zoveel mogelijk digitaal bereikbaar zijn en het streven dat er met deze overheden langs digitale weg kan worden gecommuniceerd.²⁹ Alle vragen en aanvragen moeten in digitale vorm naar de overheid kunnen worden verstuurd en omgekeerd moeten berichten van de overheid in dezelfde vorm kunnen worden ontvangen. Om dit te bereiken wordt, althans dat is de bedoeling,³⁰ in de Awb een regeling opgenomen die mogelijk moet maken dat Nederlanders, met inbegrip van Nederlanders in het buitenland en buitenlanders in Nederland, meer mogelijkheden krijgen om langs digitale weg met de overheid te communiceren. De regeling sluit wellicht aan bij de nog niet zo heel lang geleden in het Burgerlijk Wetboek opgenomen regelingen voor de totstandkoming van overeenkomsten langs elektronische weg³¹ en elektronische besluitvorming in rechtspersonen.³²

De ambities van de overheid met betrekking tot digitale beschikbaarheid en bereikbaarheid zijn niet bescheiden, maar lijken niet onhaalbaar. Het is nog niet eens zo heel lang geleden dat het enerzijds bijzonder moeilijk was geworden om een fysiek bankfiliaal te bezoeken (omdat die waren vervangen door geldautomaten, webpagina's en apps) terwijl anderzijds het telefoonmoeras van er-zijn-nog-17-wachtenden-voor-u opdoemde, vergezeld

28. Zie overw. 3 van Richtlijn 2013/37/EU van het Europees Parlement en de Raad van 26 juni 2013 tot wijziging van Richtlijn 2003/98/EG inzake het hergebruik van overheidsinformatie, *PbEU* 27.6.2013 L175/1: overwegende dat "[b]eleid voor vrije gegevensverstrekking, dat brede beschikbaarheid en hergebruik van overheidsinformatie voor privé- of commerciële doeleinden met minimale of geen juridische, technische of financiële beperkingen aanmoedigt en het circuleren van informatie zowel voor marktdeelnemers als voor burgers bevordert, kan een belangrijke rol spelen in het op gang brengen van de ontwikkeling van nieuwe diensten die gebaseerd zijn op nieuwe manieren om dergelijke informatie te combineren en in te zetten, kan de economische groei stimuleren en maatschappelijk engagement bevorderen. [...]"; zie ook *Kamerstukken II* 2014/15, 34 123, nr. 3, p. 1-2.

29. *Kamerstukken II* 2012/13, 26 643, nr. 280, p. 3-4.

30. De Minister van EZ deed aanvankelijk de toezegging het wetsvoorstel nog in 2014 naar de Kamer te sturen (*Kamerstukken II* 2013/14, 32 637, nr. 88, p. 11) maar kwam daarop later terug omdat bij de voorbereiding van de internetconsultatie van het wetsvoorstel was gebleken dat er behoefte is aan harmonisatie van beleid op het terrein van de elektronische overheid. Om deze reden is ervoor gekozen het wetsvoorstel onderdeel te laten worden van een breder integraal wetgevingsprogramma (*Kamerstukken II* 2013/14, 32 637 nr. 131, p. 1). Inmiddels is de voorbereiding van het wetsvoorstel, waarvan de werktitel is geworden Wet GDI is, overgedragen aan de Minister van BZK, die in een kamerbrief van 4 december 2015 (*Kamerstukken II* 2015/16, 26 643, nr. 373, p. 1) heeft toegezegd het wetsvoorstel in 2016 naar de Kamer te sturen. Zie ook voetnoot 43 van dit pre-advies.

31. Art. 6:227a, eerste lid, BW.

32. Art. 2:217a e.v. BW.

van de aanbeveling een bepaalde website te bezoeken. Een jaar of twee geleden hebben belangrijke spelers in het bedrijfsleven een nieuwe koers ingeslagen die, tenminste voor wie beschikt over een internetverbinding en daarvan gebruik weet te maken, een ongekende verbetering inhoudt. We hebben het over de inzet van direct chat-contact met een deskundige medewerker. Het voordeel van deze aanpak is dat de deskundige toegang heeft tot alle relevante bij zijn bedrijf geadministreerde gegevens over contract en dienstafnemer. En dat het gebruik van chat het toestaat om een deskundige medewerker in real time aan een informatietransactie of vijf tegelijkertijd te laten werken.

Dit beschikbaarheids- en bereikbaarheidsmodel is, voor zover wij overzien, begonnen bij telecomdienstverleners, maar het voorbeeld werd al snel gevolgd door banken en andere diensaanbieders die zich daarmee wensen te onderscheiden van hun concurrenten. Vanzelfsprekend slaagt niet iedere aanbieder daarin, maar al-met-al lijkt het algemeen aanvaard dat deze vorm van digitalisering inderdaad kan bijdragen aan een betere bereikbaarheid en beschikbaarheid. Ook als we onderkennen dat er geen sprake is van echte concurrentie tussen bestuursdiensten ligt voor de hand dat overheden op een zelfde wijze het contact met de burger, homo digitalis, veel beter en gebruiksvriendelijker kunnen inrichten. Wat dit betreft zijn er, als gezegd, kansen voor de ambities van Plasterk. Er zijn echter ook bedreigingen en risico's.

Er zijn op alle niveaus talloze voorbeelden van overheden die zich zijn gaan inspannen om langs digitale weg relevante informatie beschikbaar te stellen aan burgers en ondernemers. In het verlengde daarvan zien we ook dat deze overheden ernaar streven om de communicatie met burgers en ondernemers langs dezelfde digitale weg mogelijk te maken. Dit kan immers vaak ook voor deze overheden voordelen hebben, al was het maar doordat er aanzienlijke besparingen op portokosten mogelijk zijn.³³

In de visiebrief wordt verwezen naar de web portals die burgers en ondernemers in staat stellen kennis te nemen van, en zo nodig te communiceren over, de voor hun specifieke situatie relevante gegevens, met inbegrip van de op hen betrekking hebbende persoonsgegevens. Het gaat om de websites in het zgn. 'mijn-domein', waarop burgers of ondernemers inloggen om hun eigen overheidszaken te regelen. Denk aan MijnOverheid.nl, een portal die toegang biedt tot elektronische post van overheden en tot de door overheden vastgelegde persoonlijke gegevens, alsmede de stand van zaken van de bij deze overheden lopende zaken. Van MijnOverheid.nl

33. De RDW bijvoorbeeld was in 2014 goed voor iets minder dan 7 miljoen APK-keuringen (licht en zwaar) en stuurde in het kader daarvan zo een 6 miljoen geautomatiseerde brieven uit ter herinnering van het verlopen van de APK. Alleen al aan portokosten voor dit deel van de bedrijfsvoering van de dienst kunnen dus al snel enkele miljoenen worden bespaard. Zie het online-jaarverslag van de RDW: http://jaarverslag2014.rdw.nl/_layouts/Rdw.Jv2014.Portal/home.aspx (geraadpleegd 30 december 2015).

wordt gebruik gemaakt door de Belastingdienst, RDW, SVB, UWV, gemeenten en het Kadaster. Via de portal krijgt u, zo meldt startpagina, een herinnering als uw rijbewijs dreigt te verlopen. U kunt er controleren hoe u bij de gemeente geregistreerd staat of de status van een omgevingsvergunning volgen. En dat allemaal overzichtelijk, veilig en altijd beschikbaar. “*U logt gemakkelijk in met uw DigiD.*” Andere voorbeelden van zulke overheidsportals zijn Werk.nl, MijnToeslagen.nl, MijnDUO.nl en de websites van gemeenten, zoals het Servicepunt Sociaal op DenHaag.nl.

Van dergelijke web portals kunnen worden onderscheiden de websites die bedoeld zijn voor de digitale beschikbaarstelling van algemene overheidsinformatie, dat wil zeggen: de overheidsinformatie die voor iedereen relevant kan zijn. Daarbij valt te denken aan de bekendmaking van wet- en regelgeving, kennisgevingen van vergunningen, besluiten en beleidsregels, bestemmingsplannen, reglementen, regelingen, aanvraagformulieren, beleidstukken, notulen van openbare vergaderingen, brochures, enzovoorts. Voorbeelden waarmee we als praktijkjuristen vertrouwd zijn geraakt betreffen natuurlijk Overheid.nl en Rechtspraak.nl, Belastingdienst.nl etc.

3.2 Digitaal, tenzij...

Er is recent enig onderzoek gedaan naar de digitale beschikbaarheid van overheidsinformatie en de bereikbaarheid van overheden. Voor ons is vooral het onderzoek van de Nationale ombudsman van belang. Dat onderzoek ging specifiek in op de belangen van de burgers die langs digitale weg in contact proberen te treden met de overheid. We ontleen er een aantal zorgen aan over hoe de gedigitaliseerde overheid wordt vormgegeven en hoe het vanuit het perspectief van de digitale burger mis kan gaan.³⁴ Zo is een belangrijke bevinding dat voor een substantieel deel van de burgers met digitalisering het tegenovergestelde wordt bereikt van wat er wordt beoogd. Ongeveer twintig procent van de burgers heeft zoveel moeite met digitalisering dat het daardoor voor hen juist moeilijker wordt om met de overheid in contact te treden. Voor deze groep *offliners* is de digitalisering van de overheid problematisch, zeker als er geen mogelijkheid is om gebruik te maken van andere kanalen om de overheid te bereiken en als het voor hen lastig is om fouten in gedigitaliseerde systemen te herstellen.

Het rapport van de ombudsman wijst erop dat er sprake is van een ‘opvallende verschuiving in de uitgangspunten van de overheid’ over de voorwaarden die worden gesteld aan een goede gedigitaliseerde dienstverlening. In de daarvoor opgestelde gedragscode, de Burger Service Code, stond eerst de keuzevrijheid van de burger voorop. In latere beleidsstukken

34. Kanne en Van den Berg (2013).

verschoof het accent en staat dat persoonlijk contact mogelijk gemaakt wordt, als dat noodzakelijk of bevorderlijk is voor de kwaliteit van de dienstverlening. En dat wekt, aldus het rapport, de indruk dat het niet meer zozeer gaat om wat de burger wil maar om wat de overheid wenselijk acht. Een bevestiging daarvan zien we ook in het uitgangspunt van de verantwoordelijke minister dat wordt samengevat in de vuistregel ‘*digitaal, tenzij dat niet kan*’. De standaard situatie of *default-setting* is digitalisering, andere kanalen zijn de uitzondering waarvan alleen gebruik wordt gemaakt als de noodzaak daarvan wordt aangetoond.

Er is niet veel fantasie nodig om te bedenken wat er dan kan misgaan. We willen wel geloven dat de groep van minder digitaalvaardige burgers, ondanks de vergrijzing,³⁵ inmiddels in omvang mogelijk is afgenomen en nog wel verder zal afnemen. Maar ook dan kan de gedigitaliseerde overheid het zich niet veroorloven dat zij een grote groep burgers niet goed kan bereiken en dat zij daardoor niet kan worden bereikt. Het is, zolang we het hebben over deze substantiële percentages, onontkoombaar dat de digitale overheid offline kanalen blijft aanbieden. We wagen ons niet aan percentages waarbij dergelijke kanalen niet meer nodig zouden zijn, maar kunnen wel zeggen dat op dit moment beschikbaarheid en bereikbaarheid niet daarzonder kunnen. In zoverre past scepsis bij de bezuinigingen die de overheid denkt te kunnen realiseren door digitalisering. Als we niet het risico willen lopen dat een grote groep offliners wordt uitgesloten, gaat digitalisering voorlopig waarschijnlijk vooral geld kosten. Daarbij is er natuurlijk de zorg dat besparingsambities er de facto toe gaan leiden dat een grote groep minder digivaardigen wordt uitgesloten van communicatie met de digitale overheid.

Risico I. Digitalisering met besparingsambities kan ertoe leiden dat een grote groep minder digivaardigen (offline burgers en ondernemers) *de facto* wordt uitgesloten.

3.3 Een recht op DigiD?

Verband houdend met het voorgaande (en met de in het volgende hoofdstuk nog te bespreken informatieveiligheid) is dat de bereikbaarheid en beschikbaarheid van de digitale overheid afhankelijk is van middelen die door diezelfde overheid ter beschikking worden gesteld. Om met de digitale overheid te communiceren is veelal een DigiD vereist. Er vanuit gaand dat iedere burger in staat moet zijn om met die overheid te communiceren zouden we verwachten dat iedereen daarop aanspraak maakt. De regeling van DigiD lijkt daarin echter niet zonder meer te voorzien. Wie gebruik wil maken van DigiD kan dat aanvragen en om het vervolgens toegekend te

35. Loos (2010).

krijgen. Tot voor kort werd daarvoor van hem of haar verlangd dat hij of zij akkoord ging met de Gebruiksvoorwaarden DigiD.³⁶

Deze voorwaarden blonken niet uit in evenwichtigheid en bevatten maar weinig waarborgen voor de gebruiker, de digitale burger. Zo stond er dat Logius, als beheerder van DigiD de gebruiker kon uitsluiten van verder gebruik van DigiD “[b]ij (het vermoeden van) misbruik of oneigenlijk gebruik van DigiD.”³⁷ En ook dat Logius “de toegang tot het gebruik van DigiD op elk gewenst moment [kan] (doen) beëindigen of blokkeren”. En “[i]n geval van beëindiging of blokkering vervalt onmiddellijk het recht op het gebruik van DigiD.” Als het gebruik van DigiD werd beëindigd, onderbroken of geblokkeerd was het, zo bleek uit de voorwaarden, mogelijk dat “de informatie die de Gebruiker via DigiD heeft opgeslagen niet meer achterhaald kan worden.” En dat was een risico dat de gebruiker maar heeft te accepteren. “Gebruiker accepteert dit risico.”

Voorwaarden als deze zijn niet heel ongebruikelijk bij de besturingsprogrammatuur van onze smartphones of standaardsoftwarepakketten, maar misschien omdat we weten dat de afdwingbaarheid ervan beperkt wordt door het consumentenrecht kunnen we ermee leven. Anders kunnen we mogelijk met enige moeite migreren naar de een of andere alternatieve dienstverlener. Voor een overheid die uitgaat van digitale beschikbaarheid en bereikbaarheid (immers ‘*digitaal, tenzij...*’) is wel duidelijk dat dit soort voorwaarden niet meer kan. Uit openbare bronnen hebben we niet kunnen achterhalen hoe vaak een DigiD wordt geweigerd of ingetrokken, maar naar verluidt zou dat enkele honderden keer per jaar gebeuren. Wat de overwegingen daarbij waren is ook onbekend. Over de rechtsmiddelen die ertegen zouden kunnen worden ingezet hebben we wel gedachten. Een probleem ontstaat natuurlijk als een DigiD nodig is om dat te doen ...³⁸

Een min-of-meer vergelijkbare situatie zagen we ook bij de gebruiksvoorwaarden van MijnOverheid.nl en andere mijn-domeinen van de digitale overheid. Ook daarvoor was de wettelijke grondslag voor de regeling ervan nogal zwak.³⁹ Voor MijnOverheid was deze geregeld in het Besluit

36. De Gebruiksvoorwaarden DigiD van 15 mei 2012 (versie 6.0) zijn nog steeds betrekkelijk eenvoudig te vinden met een internetzoekmachine en anders op https://www.digid.nl/fileadmin/digid/downloads/20120515_gebruiksvoorwaarden_digid_versie_6_0_def.pdf (geraadpleegd 30 december 2015).

37. Art. 2.15 van de Gebruiksvoorwaarden DigiD.

38. In de MvT bij het Wetsvoorstel Vereenvoudiging en digitalisering van het procesrecht wordt als authenticatiemiddel gedacht aan DigiD voor burger, aan eHerkenning voor rechtspersonen en aan de Advocatenpas voor advocaten. Aldus *Kamerstukken II* 2014/15, 34 059, nr. 3, p. 21, 35-36, 41-42 en 59.

39. Aldus ook Overkleef-Verburg (2014) p. 321.

vaststelling aansluitvoorwaarden MijnOverheid.nl⁴⁰ en het Besluit beheer Persoonlijke Internetpagina.⁴¹

Inmiddels is één en ander geregeld in de Regeling voorzieningen GDI.⁴² In deze regeling wordt niet meer uitgegaan van door de gebruikers expliciet te geven instemming met de betreffende gebruiksvoorwaarden. Dit is omdat het gebruik van MijnOverheid.nl met de door de Wet elektronisch berichtenverkeer Belastingdienst⁴³ ingevoerde verplichte digitale aangifte niet meer plaatsvindt op basis van vrijwilligheid. Er is dus nu wel een publiekrechtelijke regeling en deze biedt als zodanig de gebruiker, homo digitalis, wel al meer waarborgen en rechtszekerheid dan de daarvoor gehanteerde gebruiksvoorwaarden. Uit de toelichting bij de regeling blijkt echter dat deze primair beoogt om de bestaande, in de praktijk reeds gehanteerde voorschriften, een wettelijke basis te geven. Daardoor zijn de gevolgen ervan, volgens de toelichting, beperkt. En we zien dan ook dat de regeling nog steeds nogal eenzijdig opgestelde voorwaarden bevat. Zo kan er 'bij het vermoeden van misbruik of oneigenlijk gebruik' de toegang tot MijnOverheid.nl of DigiD worden onderbroken of 'bij geconstateerd misbruik of oneigenlijk gebruik' de toegang tot de voorziening worden beëindigd. Er is in de regeling wel aandacht voor de beveiliging van één en ander, en voor de wijze waarop ongebruikelijke patronen kunnen worden onderkend die mogelijk duiden op misbruik of oneigenlijk gebruik.⁴⁴ Heel weinig aandacht is er echter voor de waarborgen van de burger tegen zo een onderbreking of beëindiging (zeg: de rechtsmiddelen daartegen of de maximale duur van zo een onderbreking of beëindiging etc.).⁴⁵ Dat geeft te denken.

Risico II. Het risico is dat de toegang tot steeds essentiëler wordende diensten van de digitale overheid wordt beheerst door regelingen met maar weinig waarborgen voor de gebruikers van deze diensten (de burgers)

40. Besluit vaststelling aansluitvoorwaarden MijnOverheid.nl van 4 december 2007, 249.

41. Besluit beheer Persoonlijke Internetpagina, 25 mei 2007, *Stcrt.* 2007, 102, p. 8.

42. Regeling voorzieningen GDI, *Stcrt.* 2015, 37158.

43. Wet elektronisch berichtenverkeer belastingdienst, *Stb.* 2015, 378.

44. NvT Regeling voorzieningen GDI, *Stcrt.* 2015, 37158, resp. p. 7-8 en p. 11.

45. In de kamerbrief van 4 december 2015 (*Kamerstukken II* 2015/16, 26 643, nr. 373) wordt een wet aangekondigd die een juridische basis beoogt te leggen onder wat wordt genoemd de Generieke Digitale Infrastructuur of GDI. De zgn. Wet GDI moet een bijdrage leveren aan de totstandkoming van een in de Awb vast te leggen 'recht op elektronisch zakendoen met de overheid'. Afgaand op de schets die in de brief van deze beoogde wetgeving wordt gegeven, zou het daarin niet zozeer gaan om waarborging van rechten van burgers, maar vooral om de afstemming van uitvoeringsprocessen, herkenbaarheid van overheidsdienstverlening, aansluiting bij standaarden, omschrijving van functionaliteiten, en dergelijke. We kunnen deze Wet GDI niet in onze beschouwingen betrekken, de formulering is nog niet bekend. Wel kunnen we de hoop uitspreken dat de risico's die we in dit preadvies inventariseren zijn onderkend.

3.4 *Wie bepaalt de selectie?*

Van andere orde zijn de vragen over de overheidsinformatie waarover iedereen moet kunnen beschikken en die daarom en in beginsel zonder beperkingen aan iedereen ter beschikking wordt gesteld. Een probleem is dat onduidelijk is of alle overheidsinformatie die daarvoor in aanmerking komt door de desbetreffende overheid uit eigen beweging wordt aangeboden. De verwachting lijkt gerechtvaardigd dat, mede dankzij open-data wetgeving,⁴⁶ voor de categorieën van overheidsinformatie waarvoor een markt is (zoals parlementaire stukken en wet- en regelgeving) betrekkelijk gemakkelijk kan worden gewaarborgd dat de informatie goed en volledig beschikbaar is.

Toch is daarmee niet verzekerd dat alle relevante overheidsinformatie inderdaad beschikbaar is. Van alle in Nederland geproduceerde rechtspraak werd in 2010 minder dan 3 procent via rechtspraak.nl beschikbaar gesteld. Inmiddels is dat, naar wij begrijpen, nog steeds niet meer dan enkele procenten.⁴⁷ Voor rechtspraak, die in principe in het openbaar wordt gedaan,⁴⁸ is het uitgangspunt kennelijk ‘niet digitaal, tenzij...’ Vanuit de rechterlijke macht wordt daarvoor wel als verklaring gegeven dat de niet gepubliceerde rechtspraak ‘onbetekenende zaken’ betrof (want toch ongemotiveerd of faillissementen enz.), en dat deze rechtspraak alleen maar het beeld op de wel relevante rechtspraak zou vertroebelen, of dat het veel te duur is om alles te anonimiseren, en dergelijke.⁴⁹ Deze overwegingen, hoewel uitvoerig uitgewerkt in een indrukwekkend proefschrift,⁵⁰ overtuigen ons niet – ook niet omdat zelden aandacht wordt besteed aan het verlies van de mogelijkheid tot wetenschappelijk en journalistiek onderzoek naar de rechtspraak als geheel.⁵¹ En, ook al is in 2012 vanuit de rechtspraak opgehelderd wat de publicatiecriteria zijn,⁵² dan nog komt het

46. Wet hergebruik overheidsinformatie, *Stb.* 2015, 271.

47. Er werden in 2014 ca. 31.330 uitspraken gepubliceerd via rechtspraak.nl (bron: Legal Intelligence) en uit het overzicht op p. 36 van het Jaarverslag Rechtspraak 2014 (www.jaarverslagrechtspraak.nl/verslag/productie-en-werkvoorraadontwikkeling) kan worden opgemaakt dat de ‘instroom’ in dat jaar ca. 1,8 miljoen zaken bedroeg. We leiden daaruit af dat het aantal gepubliceerde uitspraken vermoedelijk nog steeds niet meer dan enkele procenten bedraagt.

48. Art. 121 Grondwet: Met uitzondering van de gevallen bij de wet bepaald vinden de terechtzittingen in het openbaar plaats en houden de vonnissen de gronden in waarop zij rusten. De uitspraak geschiedt in het openbaar.

49. Zie de reacties op Mommers et al. (2010a), p. 2072; Philippart (2010) p. 2356 en van der Hoek (2010) p. 2357, en de reactie daar weer op van Mommers et al. (2010b), p. 2358.

50. Van Opijnen (2014), p. 151 e.v.

51. Aldus recent ook: F. Jensa, ‘Machines zijn eerder op te lichten dan mensen’, NRC 2 januari 2016

52. Zie Besluit selectiecriteria uitsprakendatabank Rechtspraak.nl, te vinden via www.rechtspraak.nl/Uitspraken-en-nieuws/Uitspraken/Paginas/Selectiecriteria.aspx

vanuit een rechtstatelijk perspectief geloofwaardiger voor dat in beginsel alle uitspraken worden gepubliceerd, en dat de vraag wat relevant of irrelevant is wordt beantwoord door de gebruiker van rechtspraak.nl (homo digitalis). Inmiddels lijken de algoritmes van zoekmachines hem heel goed in staat te stellen de belangrijke van de onbelangrijke zaken te scheiden. Het is voorts de vraag of álle rechtspraak áltijd moet worden geanonimiseerd. Bovendien kunnen, als bij de productie van uitspraken al rekening wordt gehouden met anonimiseren, de kosten daarvan waarschijnlijk substantieel worden teruggebracht.⁵³

Maar daarom gaat het niet eens. Het gaat erom dat de selectie van welke informatie wordt bekendgemaakt, en de keuze van de daarbij te gebruiken selectiecriteria, niet zouden moeten liggen bij degenen die deze informatie hebben geproduceerd. En dat is natuurlijk niet beperkt tot rechtspraak. Ook van andere overheden en overheidstoezichthouders hebben we gezien dat sommige besluiten en rapporten om onverklaarbare redenen niet, of na verloop van enige tijd niet meer, zijn te vinden op de website of in de administratie. Als daarnaar navraag wordt gedaan, al dan niet met een beroep op de Wet openbaarheid van bestuur of onder politieke druk, leidt dat soms ertoe dat het gezochte alsnog boven tafel komt.⁵⁴ Maar omdat we nou eenmaal niet weten wat we niet weten, valt niet te zeggen wat er nog meer bekend had kunnen worden gemaakt. En wat de redenen waren om iets niet openbaar te maken. Of niet gemakkelijk vindbaar te maken.⁵⁵

Risico III. Een risico voor de homo digitalis is dat digitale overheden in hun verhouding met burgers en ondernemers zich weten te onttrekken aan checks and balances door selectief hen betreffende informatie in meer of mindere mate toegankelijk te maken

3.5 *Samenvatting*

Als eerste wordt de transitie naar gedigitaliseerd bestuur (en naar ‘de’ homo digitalis) zichtbaar in de wijzen waarop de communicatie wordt gerealiseerd. Dat impliceert dat de manieren waarop overheid, ondernemer en burger beschikbaar en bereikbaar zijn veranderen. We vatten de kern van het hoofdstuk hier samen door de geïdentificeerde risico’s onder elkaar te zetten en een soms ongenueanceerde ‘sound byte’ (cursief) mee te geven om er later verkort mee te kunnen werken. Het gaat om:

53. Zie Mommers et al. (2010b), p. 2358.

54. Een sprekend voorbeeld is natuurlijk het “bonnetje” van de betaling aan Cees H., jaren geleden, dat uiteindelijk leidde tot het aftreden van twee bewindspersonen. Zie daarover o.a. A. Eigenraam, ‘What’s the deal met de deal van Cees H. en wie is Cees H.?’ *NRC* 9 maart 2015.

55. Zwenne (2009), p. 31; Persbericht: OPTA past beveiligingsniveau online-documenten aan wensen gebruikers aan, 17 juni 2009 en daarover Zwenne (2011), p. 3; Zwenne (2013), p. 67.

Risico I. Digibeten de dupe. Digitalisering met besparingsambities kan ertoe leiden dat een grote groep minder digivaardigen (offline burgers en ondernemers) *de facto* wordt uitgesloten

Risico II. Digitale dwangbuizen. Het risico is dat de toegang tot steeds essentiëler wordende diensten van de digitale overheid wordt beheerst door regelingen met maar weinig waarborgen voor de gebruikers van deze diensten (de burgers)

Risico III. Troebel in plaats van transparant. Een risico voor de homo digitalis is dat digitale overheden in hun verhouding met burgers en ondernemers zich weten te onttrekken aan checks and balances door selectief hen betreffende informatie in meer of mindere mate toegankelijk te maken.

De genoemde risico's spelen vooral doordat de digitalisering en de kennis daarover niet resulteren in gradueel veranderende communicatieprocessen die we gemakkelijk kunnen leren kennen. Het gaat met horten en stoten die niet iedereen kan bijbenen. Omdat voorts enerzijds de verwachting bestaat dat grote efficiencywinsten te behalen zijn en anderzijds de mogelijkheden zich voor de overheid voordoen om condities te bepalen waaronder (DigiD) en waarover (digitale formulieren) kan worden gecommuniceerd lijkt een speelveld te zijn ontstaan waarin de offline burger het spoor bijster kan raken en het online bestuur kansen ziet zich *de facto* te onttrekken aan toezicht.

4. Informatieveiligheid en identiteitsinfrastructuur

4.1 DigiD / eID-stelsel

In zijn visiebrief onthult Plasterk dat DigiD, met 10 miljoen aansluitingen, een basisvoorziening is geworden die de sleutel is voor digitale toegang van burgers tot de e-overheid. Er moet dan ook, vervolgt de brief, continu aandacht zijn voor veiligheidsmaatregelen, alsmede voor de kans op misbruik van bijvoorbeeld DigiD. Daarmee kan niemand het oneens zijn. Maar er is waarschijnlijk meer nodig dan dat. Een homo digitalis, ook (of juist) als die een marginaal niveau van digivaardigheid heeft, moet erop kunnen vertrouwen dat de communicatie met de overheid betrouwbaar en veilig is. In elk geval kan het niet zo zijn dat de veiligheidsrisico's daarvan eenzijdig bij de burger worden gelegd.

In dat verband wordt in de brief in één adem het “stelsel eID” genoemd. Dat doelt op een hoogwaardig authenticatiemiddel dat burgers, bedrijven en overheidsdiensten in staat moet stellen om, vanaf 2017, alle communicatie over-en-weer digitaal te kunnen doen.⁵⁶

56. *Kamerstukken II* 2013/2013, 26 643, nr. 280, p. 6.

Analogie tussen data- en wegverkeer

Informatieveiligheid lijkt op het eerste gezicht inderdaad een noodzakelijke voorwaarde om alles ‘digitaal te doen.’ Maar dat is alleen zo, wanneer we ons voorstellen dat informatieveiligheid iets is dat volkomen haalbaar zou zijn. Dat is echter niet zo (waarover later). Net zo min als ‘100% verkeersveiligheid’ een noodzakelijke voorwaarde is voor wegvervoer is ‘100% informatieveiligheid’ een noodzakelijke voorwaarde voor ‘dingen digitaal doen.’

Net zoals het aanbevelenswaard is te voorkomen dat wie beschonken is, of wie anderszins niet rijvaardig is, toch aan het verkeer gaat deelnemen, kan het verstandig zijn om onder ogen te zien of er condities bestaan waardoor iemand niet informatievaardig is (en als gevolg beter maar niet aan het informatieverkeer kan deelnemen). En net zoals het aanbevelenswaard is, voor wie aan het verkeer deelneemt, om zich aan de verkeersregels te houden en om een wet Mulder in te richten die de veelvoorkomende overtredingen beboet, kan het verstandig zijn om onder ogen te zien of er regels zijn voor het informatieverkeer die strafrechtelijk, en misschien ook bestuursrechtelijk kunnen worden overtreden en vervolgens bestuursrechtelijk worden afgedaan.

Het stellen van die vragen is niet populair en leidt onmiddellijk tot opwinning en beschouwingen over de inperking van grondrechten omdat veel informatierechten daar nu eenmaal worden gerangschikt. Maar het niet stellen, en het niet beantwoorden, van die en dergelijke vragen leidt tot het soort vruchteloze discussies over internet governance waar we nu al geruime tijd getuige van zijn en die de eigenlijke vraag uit te weg gaan: wie zorgt voor een communicatie-infrastructuur waarover een geoefende en oplettende gebruiker veilig en in vrijheid kan communiceren? En: is de zorg daarvoor een overheidstaak? En als dat zo is, wat zijn de eisen die worden gesteld aan de veiligheid van informatieverkeer over die infrastructuur? En wat is eigenlijk geoefend en oplettend gebruik? En als de zorg voor die infrastructuur geen bestuurs- of overheidsopdracht is, wat zijn dan de eisen die aan de private partijen die de infrastructuur aanbieden kunnen worden gesteld? En hoe kan worden toegezien op het naleven van die eisen?

Omdat dit soort vragen wel kunnen worden gesteld, en beantwoord, voor het wegverkeer gebruiken we ze ook als een kader om beveiliging van informatieverkeer te bezien. We gaan er daarbij van uit dat de analogie met het wegverkeer een bruikbare is, ook om na te gaan wat de risico's zijn voor een gecombineerd streven naar ‘informatieveiligheid’ én ‘alles digitaal willen gaan doen.’ We zijn ons ervan bewust dat er grote verschillen zijn, maar we denken dat de voordelen van het inzetten van een herkenbaar en werkzaam juridisch arrangement voldoende meerwaarde heeft.

We bespreken de bestuursrechtelijke risico's aan de hand van enkele citaten uit overheidsmissives. De visiebrief wijdt een paragraaf aan informatieveiligheid en een eID stelsel:

Het elektronisch contact met de overheid moet goed beveiligd zijn. De lessen uit het DigiNotarincident, maar ook na Lektoker en de recente Ddos-aanvallen op DigiD laten zien dat het beveiligen van informatie en de beschikbaarheid van de digitale dienstverlening urgent en blijvend op de agenda moeten staan.

Bestuurders en topmanagers in het openbaar bestuur moeten zich hiervan bewust zijn. Om dit bewustzijn en de kennis over informatieveiligheid bij deze groep te verbeteren en te borgen is de taskforce Bestuur en informatieveiligheid dienstverlening ingericht. Voor de komende twee jaar gaat deze taskforce de ministeries, uitvoeringsorganisaties, gemeenten, provincies en waterschappen bijstaan bij het verbeteren van hun bewustzijn van informatieveiligheid. [TK 26643, nr. 280]

Als we de gekozen vergelijking doorzetten zou de aanhef, overgezet naar het wegverkeer zo kunnen komen te luiden:

Het vervoer moet goed beveiligd te zijn. De lessen van 9/11 (2001), maar ook de brand in de Mont Blanc tunnel (1999), en de treinbommen in Spanje (2004) laten zien dat het beveiligen van verkeersroutes en de beschikbaarheid van vervoersdiensten urgent en blijvend op de agenda moeten staan. Bestuurders en topmanagers in het openbaar bestuur moeten zich hiervan bewust zijn.

Een dergelijke paragraaf gaan we waarschijnlijk als het gaat om verkeersveiligheid niet snel in het echt tegenkomen, omdat we het vanzelfsprekend vinden dat de overheid allang grote aandacht heeft, heeft gehad en zal blijven hebben voor het beveiligen van verkeersroutes en de beschikbaarheid van vervoersdiensten.

Wat uit deze exercitie zou kunnen worden afgeleid is dat leidinggevende bestuurders eigenlijk niet goed weten wat onder informatieveiligheid te verstaan, wat het maatschappelijk en economisch belang ervan kan zijn en waar de verantwoordelijkheden liggen wanneer de openbare infrastructuur om veilig te transigeren wegvalt of wordt gecorrumpeerd. Of, zoals de Onderzoeksraad voor veiligheid het in de ondertitel van het rapport over het Diginotar-drama, uitdrukte: digitale veiligheid bereikt de bestuurstafel te weinig. Op zichzelf is dit een eerste risico.⁵⁷

Risico IV. Het bestuur weet niet goed wat informatieveiligheid is, wat het maatschappelijk en economisch belang ervan kan zijn en waar de verantwoordelijkheden liggen als het echt mis gaat.

Het DigiD-drama

Misschien is het zo, dat het om een zo ingewikkeld vraagstuk gaat dat we nauwelijks van bestuurders kunnen verwachten dat ze er voldoende van

57. Onderzoeksraad voor Veiligheid (2012).

weten. Misschien is het goed om ten aanzien van die onzekerheid, en over de bijbehorende bestuurlijke dynamiek een paar kengetallen te noemen: Het zo-even genoemde kamerstuk heeft dossiernummer TK 26 643, nr. 280 en is, als gezegd van 13 mei 2013. Op 24 december 2015 had dit kamerdossier nr. 382 bereikt. Er zijn dus in 32 maanden 103 kamerstukken aan ICT gewijd, waarvan er niet minder dan 53 gaan over informatiebeveiliging of DigiD/eID (of beide). Er waren daarbij meer dan 27 bijlagen bijgevoegd, de meeste daarvan in de vorm van omvangrijke rapportages. Als er iets uit deze getallen kan worden afgeleid is het wel dat het ófwel om een onmogelijk complexe materie gaat, ófwel over een materie die als onmogelijk complex wordt voorgesteld. In zijn visiebrief bevestigt de bewindspersoon dit met het understatement dat ‘*[t]echnologische expertise [...] schaars en duur is*’.⁵⁸ Dit leidt tot een verzwaring van het eerdergenoemde risico:

Risico V. Voor bestuurders is de materie (veel te?) ontoegankelijk en bewerkelijk

En dat houdt in dat van bestuurders zou moeten worden gevraagd veel tijd en aandacht te investeren in het beter leren kennen en doorgronden van de materie. Wanneer dat achterwege wordt gelaten zouden deze twee risico’s tot heel eigenaardige gevolgen kunnen leiden, tenminste vanuit een traditioneel bestuursrechtelijk perspectief. We nemen het DigiD-drama als voorbeeld.

We ontleen daarbij onze beschrijving aan de managementsamenvatting van het rapport dienaangaande van Fox IT:

DigiNotar B.V. was founded as a privately-owned notarial collaboration in 1998. DigiNotar provided digital certificate services as a Trusted Third Party and hosted a number of Certificate Authorities (CAs) [...]. The services that DigiNotar provided included [...] issuing accredited qualified certificates that could be used as the legal equivalent of a handwritten signature ... for various Dutch eGovernment purposes. In June and July of 2011 DigiNotar suffered a breach, which resulted in rogue certificates being issued that were subsequently abused in a large scale attack in August of 2011.

Following the detection of the breach on July 19 of 2011 [...] On August 28, 2011, the content of a rogue wildcard certificate for the google.com domain was posted publicly, which had been issued by DigiNotar but which had not yet been revoked. For weeks the rogue certificate had been abused in a large scale Man-In-The-Middle (MITM) attack on approximately 300,000 users that were almost exclusively located in the Islamic Republic of Iran [...]

58. *Kamerstukken II* 2013/2013, 26 643, nr. 280, p. 7.

The investigation by Fox-IT showed that all eight servers that managed Certificate Authorities had been compromised by the intruder[...] While the approach to protecting the potential targets from this type of intrusion does not differ significantly from other threats, the range of scenarios that need to be taken into account is rapidly expanding.

Het gaat om een serieus probleem. De digitale identiteit van de Nederlandse overheid is gecorrumpeerd en is vermoedelijk in handen van een buitenlandse geheime dienst (in hackerskringen worden zowel die van de USA als die van Iran genoemd⁵⁹). Een ernstiger vertrouwensbreuk als gevolg informatie-onveiligheid van het digitale verkeer met, en onder de hoede van, de Nederlandse overheid is nauwelijks denkbaar.

Het gaat om een kwetsbaarheid waarvan het misbruik onmiddellijk had moeten zijn opgemerkt, en waarover de alarmbellen onmiddellijk hadden moet klinken om de schade zoveel mogelijk te beperken. Dat is niet gebeurd. Eerst heeft Diginotar (zonder succes) geprobeerd de zaak zelf te regelen en vervolgens heeft de Nederlandse overheid erop aangedrongen om de daartoe ingerichte protocols nog even buiten werking te houden omdat anders het digitale verkeer met de Nederlandse overheid teveel schade zou ondervinden.⁶⁰ Dit optreden werd (en wordt) overigens niet als het welbewust negeren van veiligheidsprotocols gepresenteerd, maar als een adequaat en doortastend optreden van onze overheid in een noodsituatie die wordt verondersteld niet aan haar te kunnen worden toegerekend. Het wordt tijd om met het DigiD-drama in het achterhoofd enkele van onze vragen puntsgewijs af te lopen.

- Wie zorgt voor een communicatie-infrastructuur waarover een geofende en oplettende gebruiker veilig kan communiceren? De betreffende communicatie-infrastructuur was internet. Die wordt aangeboden en verzorgd door het bedrijfsleven over een publiek netwerk. Netwerk en infrastructuur functioneerden prima.
- Wat bedoelen we dan met infrastructuur? Infrastructurele diensten zijn diensten die een platform vormen voor inhoudelijke diensten en zijn als zodanig zelf weer een infrastructuur. Dat kan dus in verschillende lagen. In dat licht bieden niet alleen internet, TCP/IP en DNS infrastructurale diensten, ook Google, Facebook en Twitter doen dat, voorts is de Diginotardienst waarbij certificaten worden uitgegeven eveneens een infrastructurale dienst (voor veilig transigeren over internet), net als de dienst (in casu van Microsoft) die de besmette certificaten had moeten intrekken.
- Wie zorgt voor de relevante infrastructurale dienst waarover een geofende en oplettende gebruiker veilig met overheidsdiensten kan com-

59. Aldus blijkt bijvoorbeeld uit de wikipedia-pagina's over 'Hack bij DigiNotar', https://nl.wikipedia.org/wiki/Hack_bij_DigiNotar (laatst geraadpleegd 21 december 2015).

60. Zie Dirkx (2012), beschikbaar onder kenmerk RAD/2012/161 op www.overheid.nl. Het bevestigt veel van onze *misgivings*.

municeren? De betreffende infrastructurele dienst identificeert overheidsdiensten als overheidsdienst op internet. Diginotar is de private partij die de dienst levert.

- Wie is civielrechtelijke aansprakelijk voor welke gevolgschade van een fout in de relevante infrastructurele dienst? Dat is afhankelijk van contracten, algemene voorwaarden en exonerationclausules tussen de dienstaanbieders en de afnemers.
- Wie is bestuursrechtelijk aansprakelijk voor welke gevolgschade van een fout in de relevante infrastructurele dienst? Dat is afhankelijk van de vraag of het civielrechtelijk ‘outsourcen’ van de infrastructurele dienst die betrouwbaar transactieverkeer met de overheid mogelijk moet maken door een bestuursrechtelijke bril een zorgvuldig besluit kan worden genoemd. Van belang zal daarbij kunnen zijn in hoeverre gebruikers als belanghebbenden tegen zo’n outsourcingbesluit zouden kunnen opkomen.
- Wie is politiek aansprakelijk voor welke gevolgschade van een fout in de relevante infrastructurele dienst? Dat is afhankelijk van de vraag hoe het corrumperen van de veilige infrastructuur voor betrouwbaar transactieverkeer met de overheid onder de politieke verantwoordelijkheid van de betreffende minister wordt geoordeeld.

We menen dat het DigiD-drama laat zien dat (1) de politieke aansprakelijkheid geen vorm kreeg (Donner kon geruisloos afmarcheren naar de Raad van State),⁶¹ dat (2) de bestuursrechtelijke aansprakelijkheid niet werd beproefd ten tijde van het outsourcingbesluit door partijen die later direct werden getroffen door het tijdelijke uitvallen van de infrastructuur en dat (3) de civielrechtelijke aansprakelijkheid is vervaagd in het faillissement van Diginotar en dat (4) de (mogelijke) schade die werd geleden door Iraniërs wier vertrouwelijke berichtenverkeer door hun geheime dienst werd onderschept zich aan ons blikveld onttrekt.

We menen dat hiermee enkele belangrijke risico’s zijn aangestipt:

Risico VI. De politieke en bestuursrechtelijke aansprakelijkheid rond informatiebeveiliging en eID is niet eenvoudig te realiseren

Wat hier een rol lijkt te spelen is de mate waarin beveiligingstechniek voor bestuurders en ambtenaren als een belemmering wordt ervaren om duidelijk stelling te nemen en aansprakelijkheden toe te delen en te aanvaarden. Mogelijk wordt gezichtsverlies gevreesd. Het lijkt erop dat onze bestuursrechtelijke gewoontes en cultuur niet zijn opgewassen tegen de tendens om

61. Inmiddels is de Minister van BZK op grond van art. X van de Wet elektronisch berichtenverkeer belastingdienst jo. art. 6 van de Regeling voorzieningen GDI verantwoordelijk voor de veiligheid en betrouwbaarheid van o.a. MijnOverheid.nl en DigiD.

gezag te ontleen aan technologische scholing in plaats van aan de waarneming en duiding van maatschappelijke verhoudingen. We menen dat de bedorven verhoudingen tussen bestuursdiensten en de ICT-sector, zoals die aan het licht treden in de voortdurende reeks mislukkende ICT-projecten die door overheidsdiensten worden aanbesteed,⁶² een aanwijzing zijn voor hoe moeilijk het kennelijk is om hierin verbetering aan te brengen.

Risico VII. De bestuursrechtelijke zorgvuldigheid bij (naar achteraf blijkt) relevante besluiten kon niet (of nauwelijks) ter discussie worden gesteld op het geëigende moment.

Dit vierde risico lijkt ons mede een gevolg van hoe het bij het verhelderen van politieke verantwoordelijkheid is misgelopen (als boven aangegeven). In een zich op basis van technologische innovatie voortdurend specialiserende wereld is het onvermijdelijk dat besluiten worden genomen over wat wel en wat niet kan worden geoutsourced aan het gespecialiseerde bedrijfsleven (of kan worden ondergebracht in een bijzondere civielrechtelijke organisatievorm waarin het bedrijfsleven en het bestuur samenwerken). Daarbij moet steeds de vraag onder ogen worden gezien of het besluit tot outsourcen een bestuursrechtelijk besluit is dat dient te voldoen aan de eisen die de Awb daaraan stelt – en zo ja, of die zorgvuldigheid tot uitdrukking komt in de arrangementen die rond dat besluit worden bepaald. En ook moet daarbij worden nagedacht over wie als belanghebbenden kunnen gelden en van het voorgenomen besluit op de hoogte worden gesteld c.q. in staat moeten worden gesteld hun visie te geven.

Risico VIII. De civielrechtelijke risico's rond informatiebeveiliging kunnen vergaand worden geminimaliseerd via exonatieclausules

Als het derde en vierde risico zich hebben laten gelden kan dit vijfde risico, dat immers een standaardvorm is waarin de civielrechtelijke aansprakelijkheden tussen ondernemingen worden geregeld, het lek vormen waardoor aansprakelijkheden en verantwoordelijkheden weglopen.

4.2 DDoS aanvallen en botnets

Het komt ons voor dat we in het kader van bestuursrechtelijke risico's rond informatiebeveiliging moeilijk voorbij kunnen gaan aan wat DDoS aanvallen worden genoemd. Het gaat dan om via botnets uitgevoerde aanvallen, gelijktijdig, als het tegenzit door honderdduizenden gehackte machines, op

62. *Kamerstukken II* 2014/15, 33 326, nr. 5. www.tweedekamer.nl/sites/default/files/field_uploads/33326-5-Eindrapport_tcm181-239826.pdf

een doelwit waarvan, daardoor, de communicatiecapaciteit wordt verlamd, soms voor langere tijd.

Een overheid die de ambitie heeft om ‘alles digitaal te gaan doen’ moet zijn houding bepalen ten aanzien van deze risico’s. De causale keten die dergelijke risico’s in het leven roept begint bij een kwaadwillende. De activiteiten van zo een kwaadwillende zijn weliswaar strafrechtelijk te kenmerken, maar daarmee is het risico op de verstoring van de door de overheid gebruikte informatie-infrastructuur niet uitgebannen. Opnieuw doet zich de vraag voor naar de bestuurlijke zorgvuldigheid van de digitale overheden die besluiten om hun toegankelijkheid en vermogen tot dienstverlening geheel laten verlopen via een infrastructuur waarvan de kwetsbaarheid (via aanvallen van botnets) reëel is en van tevoren als zodanig vaststaat, vooralsnog zonder uitzicht op een effectieve oplossing.

De tweede schakel in de causale keten wordt gevormd door de individuele computergebruikers die met behulp van malware worden gehackt en waarvan de gehackte (gekaapte) computers worden gebruikt om de aanvallen uit te voeren. Mogelijk zou het aantal computers dat kan worden gehackt worden beperkt door eisen te stellen aan de vaardigheden van wie aan het digitale verkeer deelnemen. Die weg naar een oplossing lijkt evenwel om veel redenen onhaalbaar. Van belang zijn hier bijvoorbeeld de vaststelling dat de doorsnee homo digitalis wél de vaardigheden heeft om apparatuur en programmatuur effectief te gebruiken, maar onvoldoende om die te kunnen beschermen tegen hacking en malware infecties. Daarbij komt dan dat beschermingsmaatregelen tegen hacking en malware onvermijdelijk een beperking inhouden van (en daarmee: een *chilling effect* kunnen hebben op) verworven informatievrijheden (zoals rechten op toegang tot informatie en de vrijheid van meningsuiting). We menen dat, ook gelet op de maatschappelijke discussie rond filteren van het internet, het van belang is vast te stellen dat het politieke klimaat rond grondrechtelijke informatievrijheden vooralsnog het verplicht stellen van essentiële beheersvaardigheden en beheerstaken onmogelijk maakt.⁶³ Ook dit is een risico.

Risico IX. Het voor een verantwoord gebruik van de digitale overheidsdienstverlening vereiste niveau van digitale beheersvaardigheden wordt de facto niet gehaald, en kan ook niet worden geëist van de offline burger omdat dat in strijd wordt geacht met verworven informatievrijheden.

Risico X. Dit impliceert een risico voor hacking en botnets en daarmee ook voor de informatieveiligheid van communicatie tussen burgers en overheden en tussen overheden onderling.

63. En één van de andere redenen die hier een rol zouden kunnen spelen wordt misschien wel – vergeef ons dit wantrouwen – gevormd door de voordelen die door opsporingsdiensten worden ervaren wanneer informatiediensten niet al te sterk zijn beveiligd.

Juist die onhaalbaarheid leidt ertoe dat we ons zullen moeten zien te redden in een wereld waarin een hoge vorm van informatieveiligheid vooralsnog niet bestaat. De voortdurende reeksen van onthullingen van via hacking of phishing illegaal en illegitiem verkregen verzamelingen creditcard- en logingegevens ondersteunt deze stelling. Er is bovendien inmiddels een beveiligingsindustrie ontstaan die rond het opsporen en vervolgens verhelpen van zogenoemde *vulnerabilities* zijn eigen infrastructurele diensten aanbiedt, een industrie die er onder de huidige condities dan ook geen belang bij heeft dat het aantal vulnerabilities volledig verdampt.

Overigens, veelal wordt als vanzelfsprekend aangenomen dat de risico's rond digitale beheervaardigheden voor de online bestuurder niet bestaan. Het DigiD-drama, en naar wij menen ook de extreem hoge faalpercentages van ICT-projecten van de overheid,⁶⁴ laten echter zien dat het geenszins om een bagatelrisico gaat.

Tenslotte. Een zeer voor de hand liggende aanpak van het als zesde genoemde risico kan erin worden gevonden om de zorg voor beheerkritische taken over te dragen aan infrastructurele dienstverleners.⁶⁵ Die tendens wordt al wel zichtbaar (bijvoorbeeld bij DigiD), met name waar het gaat om diensten die worden verwezenlijkt via wat de 'cloud' wordt genoemd. Maar clouddiensten leiden weer tot nieuwe risico's die samenhangen met asymmetrieën die de informatieverhoudingen op geheel eigen wijze kunnen verstoren. Een overheidsdienst die een infrastructurele beheerdienst uitbesteedt (outsourcet), bindt zich aan de eisen die de dienst stelt. Dat hoeft niet altijd overeen te stemmen met autonome taakvervulling. En bovendien: hierbij dient zich weer het risico aan van machtsmisbruik jegens de overheid door de dienstverlener, als randverschijnsel van het outsourcen aan clouddiensten door het bestuur. Dit risico is nog niet helder te duiden. Daarvoor is het op het moment nog te onzeker hoe de risico's van *lock-in* en van bijbehorende kennisasymmetrieën tussen opdrachtgevende bestuursdiensten en technisch geavanceerde dienstverleners kunnen worden begrepen en beheerst. Gelet op wat over grote overheidsprojecten op het gebied van de ICT boven tafel komt zijn we er niet erg gerust op.⁶⁶

64. Kamerstukken II 2014/15, 33 326, nr. 5. http://www.tweedekamer.nl/sites/default/files/field_uploads/33326-5-Eindrapport_tcm181-239826.pdf

65. Maar het betreffende risico is ook civielrechtelijk geen bagatelrisico. Per 21 september 2015, bijvoorbeeld, werd ons vertrouwen in hoogwaardige beheervaardigheden bij belangrijke commerciële infrastructurele diensten ernstig geschaad. Toen werd bekend dat door een hack in veelgebruikte ontwikkelsoftware (die wordt gebruikt om iOS apps (Apple apps) te bouwen) de gebouwde apps worden voorzien van een zogenoemde 'back doors.' De hack heeft geruime tijd ongemerkt zijn gang kunnen gaan.

66. Zie voor de ICT-faalprojecten bij de rijksoverheid weer: Kamerstukken II 2014/15, 33 326, nr. 5. http://www.tweedekamer.nl/sites/default/files/field_uploads/33326-5-Eindrapport_tcm181-239826.pdf en voor de ICT-problemen bij lokale overheden de berichtgeving in NRC, zoals: D. Stokmans, 'PinkRoccade en Centric misbruiken marktmacht' en 'Gegijzeld door de softwareboer' NRC 17 oktober 2015.

4.3 Samenvatting

De transitie naar gedigitaliseerd bestuur (en de evolutie naar de homo digitalis) wordt zichtbaar in de wijzigingen die optreden in het verwezenlijken van betrouwbare communicatie. Daarbij zijn van belang een veilige communicatie-infrastructuur en betrouwbare mechanismen waarmee de identiteit van de deelnemers kan worden vastgesteld en bevestigd. Dat blijken in de digitale wereld ingewikkelde en ook organisatorisch moeilijk te realiseren vereisten te zijn.⁶⁷

We vatten weer samen met behulp van de gesignaleerde risico's.

Risico IV. Professioneel bestuur op basis van onwetendheid. Het bestuur weet niet goed wat informatieveiligheid is, wat het maatschappelijk en economisch belang ervan kan zijn en waar de verantwoordelijkheden liggen als het echt mis gaat.

Risico V. Complexiteit van materie. Voor bestuurders is de materie (veel te?) ontoegankelijk en bewerkelijk

Risico VI. Bestuurlijke aansprakelijkheid glipt weg. De politieke en bestuursrechtelijke aansprakelijkheid rond informatiebeveiliging en eID is niet eenvoudig te realiseren

Risico VII. Bestuurlijke zorgvuldigheid post hoc. De bestuursrechtelijke zorgvuldigheid bij (naar achteraf blijkt) relevante besluiten kon niet (of nauwelijks) ter discussie worden gesteld op het geëigende moment.

Risico VIII. Exoneratievergiert. De civielrechtelijke risico's rond informatiebeveiliging kunnen vergaand worden geminimaliseerd via exoneratieclausules

Risico IX. Beheersvaardigheid is informatiefiltering. Het voor een verantwoord gebruik van de digitale overheidsdienstverlening vereiste niveau van digitale beheersvaardigheden wordt de facto niet gehaald, en kan ook niet worden geëist van de burger, omdat dat in strijd wordt geacht met verworven informatievrijheden.

Risico X. Informatievrijheid impliceert botnets. Dit impliceert een risico voor hacking en botnets en daarmee ook voor de informatieveiligheid van communicatie tussen burgers en overheden en tussen overheden onderling.

Informatieveiligheid is dus moeilijk en ingewikkeld, zeker ook als het gaat om infrastructurele informatiediensten waarmee burgers en bestuurders zichzelf in een digitale omgeving identificeren en authenticeren. Voldoende ervan weten is voor bestuurders en voor burgers vaak een brug te ver. Als gevolg is er vanuit de bestuurszijde nogal eens een streven, meestal effectief, gericht op het minimaliseren van verantwoordelijkheden. De besluiten van de digitale overheden om werkzaamheden of verantwoordelijkheden uit te besteden (outsourcing) zijn zelden bij belanghebbenden bekend en worden niet steeds ingebed in een praktijk van continu, toereikend toe-

67. In aanvulling op het DigiD-drama openbaren zich op het moment van schrijven twee corruptieschandalen rond handel in politieke informatie en in douane-autorisaties – en het aantal ontdekte corruptiegevallen bij de politie baart zorgen, meldt de NOS (<http://nos.nl/artikel/700526-politie-verdacht-van-corruptie.html>) .

zicht. Als gevolg wordt de schade die kan ontstaan door misbruik van onveilige infrastructurele diensten doorgaans op de burger afgewenteld – we zagen dat al in hoofdstuk 3 van dit preadvies. Opmerkelijk is dat beheerkennis bij zowel burger als bestuurder achterblijft, wat de kans op onveilige infrastructuur doet toenemen (botnets), en/of de autonomie van de overheid bij outsourcecontracten aan (onwenselijke) beperkingen kan binden. Het lijkt erop dat de risico's van onveilige infrastructuur in de huidige bestuursrechtelijke praktijk niet transparant zijn en dus evenmin effectief kunnen worden beheerst.

5. Overheidsgegevensgebruik

5.1 Het gebruik van digitale gegevens binnen en door de overheid

In de visiebrief wordt uiteengezet dat de digitale overheid meer en beter gebruik moet gaan maken van de beschikbare digitale gegevens. Dit omdat – we parafraseren de brief – het voor de burger onbegrijpelijk is dat hij of zij aan de overheid elke keer dezelfde gegevens moet doorgeven. En ook omdat overheidsorganisaties niet aansluiten bij gemeenschappelijk ontwikkelde voorzieningen, zoals de basisregistraties en MijnOverheid, wat onnodig veel tijd en ergernis kost en voor de overheid als geheel onnodig ook nog eens duur is.⁶⁸

Voor Plasterk gaat het dus om het vergroten van het gebruiksgemak voor de burger en het efficiënter en betrouwbaarder maken van de overheidsbedrijfsvoering. De overheid moet de burger niet steeds weer dezelfde gegevens vragen. De burger verwacht 'één overheid' en 'daarbij hoort eenduidigheid en hergebruik van generieke voorzieningen'. Ook om redenen van consistentie, veiligheid en stabiliteit is het beter als binnen de overheid gebruik wordt gemaakt van dezelfde voorzieningen en infrastructuur, basisregistraties en gegevensuitwisseling.

Het gaat echter niet alleen over gebruiksgemak, efficiëntie, betrouwbaarheid en kostenbesparingen. Andere kamerstukken laten zien dat het verbeteren van het overheidsgegevensgebruik ook wordt gerelateerd aan controle en toezicht op burgers, en andere meer repressieve doelstellingen. Het meer en beter gebruik maken van digitale gegevens moet ook worden gezien in het kader van het mogelijk maken van gegevensuitwisseling, tussen overheden en met private partijen, om toe te zien op de naleving van allerlei wet- en regelgeving. Het gaat dan, bijvoorbeeld, om de bestrijding van belastingfraude en het tegengaan van misbruik en oneigenlijk gebruik van overheidsvoorzieningen en -toeslagen, en allerlei andere vormen van fraude en criminaliteit, zoals daar zijn: illegale hennepcultuur, vastgoedfraude

68. *Kamerstukken II* 2013/2013, 26 643, nr. 280, p. 7.

de, verzekeringsfraude, zorgfraude, alsmede milieucriminaliteit, cybercrime en voertuigcriminaliteit, zelfs snelheidsovertredingen.

Vaak vindt deze gegevensuitwisseling plaats binnen samenwerkingsverbanden van overheden en anderen. De bedoeling is dat de gegevens waarover ieder van de deelnemers beschikt met elkaar in verband kunnen worden gebracht voor gemeenschappelijke analyses. Wat daarbij als praktisch probleem wordt opgevat is dat de onderliggende wetgeving, op basis waarvan de onderscheiden deelnemers over de relevante gegevens kunnen beschikken, in veel gevallen eraan in de weg staat dat deze gegevens kunnen worden gedeeld met andere deelnemers aan het samenwerkingsverband. Om dit op te lossen wordt een Kaderwet gegevensuitwisseling voorgesteld. Er moet daarmee worden voorzien in een generieke grondslag voor de gegevensverstrekking aan samenwerkingsverbanden en mogelijk maken dat gebruik kan worden gemaakt van ‘moderne analysetechnieken als datamining en profiling’. En daarmee kan bijvoorbeeld een lijst worden gegenereerd van de personen ten aanzien waarvan wordt vermoed dat er sprake is van een bijzonder groot risico dat zij fraude plegen. Of, het staat er echt, dat zij vermoedelijk *gaan* plegen.⁶⁹

5.2 De Kaderwet gegevensuitwisseling

Er is nog geen Kaderwet gegevensuitwisseling, en omdat daarop nogal wat kritiek is geuit,⁷⁰ moeten we nog zien of die er in de vorm die is voorgesteld gaat komen. Met de inwerkingtreding van het SyRI-besluit⁷¹ op 12 september 2014 is er wel al de mogelijkheid dat gemeentebesturen, bestuursorganen of sociale zekerheids- of belastingtoezichthouders een samenwerkingsverband aangaan dat is gericht op het voorkomen en bestrijden van onrechtmatig gebruik van overheidsvoorzieningen op het terrein van de sociale zekerheid en inkomensafhankelijke regelingen en

69. In de brief waarin de verkenning van de Kaderwet gegevensuitwisseling aan de Tweede Kamer wordt aangeboden (*Kamerstukken II* 2014/15, 32 761, nr. 79) wordt inderdaad gezinspeeld op ‘predictive policing’, getuige deze opmerkingen: “[Er is] het voornemen een profiel van beroepsfraudeurs te ontwikkelen, maar zou het zo’n profiel op basis van de huidige wetgeving niet kunnen matchen met alle data waarover zij rechtmatig de beschikking heeft. Hierdoor kan er geen lijst gegenereerd worden van personen met een bijzonder groot risico dat zij fraude (gaan) plegen.” In de fiscale vakliteratuur werden al eerder methodes besproken gericht op het ‘construeren van patronen op basis van (potentiële) toekomstige gedragingen’ en het ‘conceptualiseren van toekomstige non-compliance gedragspatronen’, zie: Berkhout en Van Engers (2012). In één en ander zien we hoe enthousiast wordt voorgesteld op de donkere science fiction wereld van Steven Spielberg’s *Minority Report* (Dreamworks SKG/20th Century Fox 2002).

70. Zie bijv. de brief van het Cbp aan de Minister van Veiligheid en Justitie van 25 februari 2015, kenm. z2015-00155; Martijn en Goslinga (2015).

71. Besluit van 1 september 2014 tot wijziging van het Besluit SUWI in verband met regels voor fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens met inzet van SyRI, *Stb.* 2014, 320.

dergelijke. In het kader van dit samenwerkingsverband kunnen op grond van het SyRI-besluit maar liefst zeventien categorieën van gegevens (zoals: arbeidsgegevens, detentiegegevens, gegevens over roerende en onroerende goederen, inburgeringsgegevens, nalevingsgegevens, onderwijsgegevens, pensioengegegevens, re-integratiegegevens, schuldenlastgegevens, etc.) worden gekoppeld en vervolgens geanalyseerd, om zogeheten ‘risicomeldingen’ te genereren.⁷²

Zo een risicomelding geeft aan dat een rechtspersoon of een natuurlijk persoon ‘onderzoekswaardig’ wordt geacht in het licht van de doelstellingen van het betrokken samenwerkingsverband.⁷³ De gegenereerde risicomeldingen worden aan de betreffende bestuursorganen en personen van het samenwerkingsverband verstrekt, voor zover deze voor hen relevant zijn. Op verzoek kunnen de risicomeldingen ook worden verstrekt aan het OM en de politie, voor zover dat noodzakelijk is voor de uitvoering van hun wettelijke taken.⁷⁴

Voor de homo digitalis betekent dit dat de analyses die eerst niet konden worden gedaan, of alleen grotendeels handmatig in een beperkt aantal specifieke gevallen en waarschijnlijk alleen door een beperkt aantal deskundigen, als gevolg van digitalisering nu met aanmerkelijk minder moeite en veel vaker kunnen worden gedaan. Een door de Raad van State aangeduid risico daarbij is dat de categorieën van te verwerken gegevens nogal ruim en veelomvattend zijn omschreven en diep kunnen ingrijpen in iemands persoonlijke levenssfeer: *“De opsomming van gegevens is weliswaar”, zo zegt het adviescollege het in zijn advies over het ontwerpbesluit, “bedoeld om de gegevensverwerking in te perken (dataminimalisatie), maar is in feite zo ruim dat er nauwelijks een persoonsgegeven te bedenken is dat niet voor verwerking in aanmerking komt.”* Dat is nogal wat. Ook al wordt bij ieder afzonderlijk project en samenwerkingsverband nader bepaald welke gegevens daarvoor nodig zijn, dan nog is daarmee het risico van sleepnet-acties (*fishing expeditions*) helemaal niet weggenomen.⁷⁵

72. Art. 5a.1, derde lid, onder a t/m q, Besluit SUWI, het gaat in alfabetische volgorde om achtereenvolgens: arbeidsgegevens, gegevens inzake bestuursrechtelijke maatregelen en sancties, detentiegegevens, fiscale gegevens, gegevens over roerende en onroerende goederen, handelsgegevens, huisvestingsgegevens, identificerende gegevens, inburgeringsgegevens, nalevingsgegevens, onderwijsgegevens, pensioengegegevens, re-integratiegegevens, schuldenlastgegevens, uitkerings- toeslagen- en subsidiegegevens, vergunningen en ontheffingen, en zorgverzekerings-gegevens. Zie daarover T, Wieringa (2015).

73. NvT bij SyRI-besluit, *Stb.* 2014, 320, p. 14, 21-24.

74. Zie resp. art. 65, derde lid, onderdelen a en b, Wet SUWI; NvT bij SyRI-besluit, *Stb.* 2014, 320, p. 15

75. Advies Raad van State, nr. W12.14.0102/III, 's-Gravenhage, 15 mei 2014, *Stcrt.* 2014, nr. 26306.

Het Nader Rapport bij het besluit gaat daarop wel in maar stelt niet gerust. Er wordt opgemerkt dat de desbetreffende gegevens op grond van andere regelingen ook al aan gemeenten of UWV en Svb moeten worden verstrekt⁷⁶ en dat het niet wenselijk is om op voorhand gegevens uit te sluiten, omdat SyRI-projecten zich kunnen richten op verschillende thema's. De vereiste dataminimalisatie⁷⁷ moet worden gewaarborgd doordat de samenwerkingsverbanden die gebruik maken van SyRI geacht worden zelf te toetsen welke gegevens nodig zijn voor het welbepaalde en nadrukkelijk omschreven doel van de samenwerking, dat weer moet passen binnen de in de wet genoemde doelen van het tegengaan van onrechtmatig gebruik van overheidsmiddelen en overheidsvoorzieningen op het terrein van sociale zekerheid en inkomensafhankelijke regelingen, het bestrijden van belasting- en premiefraude en niet naleving van arbeidswetten.⁷⁸

Al met al lijken de waarborgen die de wet biedt betrekkelijk. Een samenwerkingsverband dat gebruik wil maken van SyRI moeten binnen de ruime wettelijke kaders voor zichzelf de beperkingen stellen waarbinnen de gegevensanalyse mag plaatsvinden. En de vraag is dan natuurlijk of we erop kunnen vertrouwen dat deze samenwerkingsverbanden, die worden aangegaan om heel uiteenlopende vormen van fraude en misbruik te bestrijden, bereid zijn zichzelf daarbij inderdaad gebruiksbeperkingen op te leggen. Er is, menen wij, een risico dat deze samenwerkingsverbanden niet vanzelfsprekend geneigd zijn het belang van fraudebestrijding ondergeschikt te maken aan de bescherming van de persoonlijke levenssfeer van degenen over wie gegevens kunnen worden verwerkt. En dat is een risico dat toeneemt als deelnemers aan het samenwerkingsverband per saldo veel te winnen hebben, of denken te hebben, bij de analyse en maar weinig bij de bescherming van de persoonlijke levenssfeer.

Risico XI. Als het gaat om gegevensgebruik door en binnen de overheid is de wetgever maar in beperkte mate geneigd te voorzien in beperkingen met betrekking tot gegevensuitwisseling en gegevensanalyse.

Één en ander roept natuurlijk ook vragen op met betrekking tot rechtsbescherming van burgers, en meer in het bijzonder de waarborging van de onder meer in het Europees Handvest vastgelegde recht op gegevensbe-

76. O.g.v. resp art. 64 Wet werk en bijstand art. 54 Wet Structuur uitvoeringsorganisatie werk en inkomen.

77. Art. 11 Wbp.

78. Zie Nader Rapport, opgenomen bij de publicatie van Advies Raad van State inzake het ontwerpbesluit houdende regels voor fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens (Besluit SyRI), *Stcrt* 2014, nr. 26306.

scherming.⁷⁹ Ook is er de vraag in hoeverre de overheid voldoet aan de strenge voorwaarden die worden gesteld, en straks in de nieuwe Europese privacyregels⁸⁰ gaan worden gesteld, aan risicoprofilering. In haar bespreking van de verhoudingen tussen belastingdienst en digitale burger stelt Overkleef-Verburg dan ook onomwonden dat “*de rechtmatigheid [van deze risicoprofilering] derhalve vooralsnog aan twijfel onderhevig [blijft]*”.⁸¹

Risico XII. Als het gaat om gegevensgebruik door en binnen de overheid is de wetgever maar in beperkte mate geneigd rekening te houden met beperkingen verband houdend met fundamentele rechten en vrijheden, zoals die waarin het Europees Handvest voorziet.

Voor de digitale overheid is er daarmee het risico dat deze SyRI- en andere wetgeving, en de daarop gebaseerde gegevensuitwisselingssystemen en -arrangementen, geen stand blijken te kunnen houden.⁸² Dat dit geen denkbeeldig risico is kan wellicht worden opgemaakt uit het voorbeeld van de Wet bewaarplicht telecomgegevens, die vanwege strijdigheid met artikel 7 en 8 van het Handvest buiten werking werd verklaard nadat het Hof van Justitie al eerder de daaraan ten grondslag liggende Richtlijn 2006/24/EC ongeldig had verklaard.⁸³ Een ander, recenter voorbeeld is de ongeldigverklaring van het Safe Harbor-besluit van de Europese Commissie op grond waarvan persoonsgegevens konden worden doorgegeven naar ondernemingen in de Verenigde Staten.⁸⁴

Risico XIII. De wetgeving waarin te weinig rekening wordt gehouden met de bescherming van fundamentele rechten en vrijheden is kwetsbaar en loopt het risico door een rechter buitenwerking te worden gesteld. Voor de op basis daarvan gebouwde gegevensuitwisselingssystemen is dit een potentiële faalfactor.

Weer ander risico ligt in het vermoeden dat digitale bestuurders, binnen de door de wetgever toch al ruim gestelde kaders, de neiging hebben om de grenzen op te zoeken van wat toelaatbaar is, en daar nogal eens overheen gaan. Een voorbeeld daarvan zagen we bij de aanleg door de belastingdienst van een verzameling met de inkomensgegevens van alle huurders in Nederland ten behoeve van de uitvoering van de regeling met betrekking

79. Art. 8 van Handvest van de Grondrechten van de EU (2007/C 303/01), PbEG 2007, C 303/1.

80. Zie art. 20 van de General Data Protection Regulation (consolidated compromise text of December 15th, 2015).

81. Overkleef-Verburg (2014), p. 318.

82. Zwenne and Steenbruggen (2015).

83. Resp. HvJEU 8 april 2014, C-293/12 en C-594/12 en vz Rb Den Haag, 1 maart 2015, ECLI:NL:RBDHA:2015:2498.

84. HvJEU 6 oktober 2015, C-362/14.

tot de inkomensafhankelijke huurverhoging in het kader van het tegengaan van scheefwonen. In de gegevensverzameling werden gemakshalve ook de gegevens opgenomen van huurders in de vrije sector die niet onder de regeling vallen.⁸⁵ Een ander voorbeeld zagen we in het gebruik van de gegevens die de ene overheidsorganisatie niet meer mag bewaren, maar die nog wel beschikbaar zijn bij een andere overheidsorganisatie, als in: de kentekengegevens die de politie na vier weken moet verwijderen, maar die de politie vervolgens nog wel zonder veel moeite kan verkrijgen bij de belastingdienst.⁸⁶

In deze voorbeelden zien we dat er weinig betekenis wordt toegekend aan het beginsel van dataminimalisatie en het daarmee verband houdende uitgangspunt dat er selectie moet plaatsvinden voordat er wordt verzameld (*'select-before-you-collect'*). Alles wordt verzameld en pas dan wordt gezien wat door de desbetreffende overheid kan worden gebruikt. We hebben het dan over sleepnet-acties (*'fishing expeditions'*). En daarbij speelt ook het doelbindingsbeginsel, dat verlangt dat gegevens niet mogen worden verwerkt voor doeleinden die onverenigbaar zijn met het doel waarvoor ze zijn verzameld, geen rol van betekenis meer.

Risico XIV. Digitale bestuurders hechten weinig betekenis aan beginselen als select-before-you-collect en hebben weinig moeite met sleepnet-acties, als die effectief lijken om de door hen gestelde doelen te bereiken.

Waar gaat het naar toe? We kunnen ons een voorstelling proberen te maken van wat het voorgaande gaat betekenen in een wereld waarin exponentieel meer gegevens dan thans gaan worden vastgelegd, omdat er nu eenmaal steeds meer digitaal wordt gedaan en gemaakt (*datafication*).⁸⁷ De digitale sporen daarvan kunnen worden gebruikt, en gaan waarschijnlijk zonder nadere maatregelen ook inderdaad worden gebruikt door overheden die daarover kunnen beschikken op basis van bevoegdheden die zijn gemaakt in (en: voor) een offline wereld. We hebben het over de gegevens die zijn te vinden in de systemen die worden gebruikt voor wat wordt aangeduid als het internet-van-dingen (*Internet-of-Things* of *IoT*), smart-cities, quantified communities en dergelijke. Denk dan aan: de kwartierwaarden uit slimme energiemeters, huisthermostaatgegevens, locatiegegevens van smartphones, sensoren in de fietsenstalling, de sentimenten die zijn af te leiden uit social media, online boodschappenlijstjes, rijgedraggegevens uit autonavigatieapparaten en interconnected auto's, lichaams-temperatuur- en hartslaggegevens, 'wearables', etc.

85. Cbp Rapport Onderzoek Belastingdienst - aanpak scheefwonen, 5 februari 2014 te vinden via <https://cbpweb.nl/nl/nieuws/cbp-belastingdienst-gebruikte-inkomensgegevens-strijd-met-de-wet> (geraadpleegd 1 januari 2016).

86. Martijn (2014).

87. Mayer-Schönberger and Cukier (2013).

We kunnen dat niet los zien van de digitalisering ten behoeve van het verbeteren van de beschikbaarheid van overheidsinformatie en de bereikbaarheid van overheden (hoofdstuk 2 van dit preadvies). We denken daarbij bijvoorbeeld aan de digitale aangifte, bijvoorbeeld via een aangifte-app op tablet. Zo een digitale aangifte stelt de belastingdienst in staat om niet alleen te beschikken over de door aangifteplichtigen verstrekte gegevens, maar ook over gegevens betreffende de wijze waarop het digitale aangifteformulier is ingevuld. We kunnen dan denken aan de snelheid waarmee en de volgorde waarin de verschillende vragen zijn beantwoord, de tijd die de beantwoording van bepaalde vragen heeft gekost, de verbeteringen die op verschillende momenten zijn aangebracht, het aantal toetsaanslagen per minuut, locaties waar het biljet werd ingevuld, het taalgebruik, etc. Voor een belastingdienst die uitgaat van ‘een informatiegestuurde subject-gerichte handhavingsregie’ en het streven om ‘iedere belastingplichtige de behandeling te geven die hij verdient’,⁸⁸ zijn daaruit ongetwijfeld bruikbare signalen af te leiden. Het is niet onaannemelijk dat er bij de belastingdienst op zijn minst de wens is van die signalen gebruik te maken bij de controle van de aangifte.⁸⁹

Ook als we ons beperken tot de gegevens waarover de overheid nu al beschikt, of zonder al teveel moeite kan beschikken, is duidelijk dat de burger meer dan ooit te voren door de overheid wordt gekend, door middel van sms-perkeergegevens, trajectcontroles, ov-chipkaartgegevens, sociale media-berichten, smartphonelocaties, televisiekijkgedrag, etc. Een digitale overheid kan, als de wet of rechter daaraan geen beperkingen stelt, in niet eerder vertoonde mate inzicht hebben in haar digitale burgers. Omdat dit leidt tot meer mogelijkheden om gedrag van digitale burgers en ondernemingen te beïnvloeden of te sturen, kan dat op zichzelf, menen wij, als risico worden geduid. Er is sprake van een uitbreiding van (nieuwe) machtsinstrumenten en dwangmiddelen, zonder dat duidelijk is in hoeverre daar passende waarborgen tegenover staan.

Risico XV. Er komen heel veel meer gegevens beschikbaar die door digitale overheden kunnen worden gebruikt, en waarschijnlijk ook gaan worden gebruikt, om macht uit te oefenen over burgers en ondernemers, zonder dat duidelijk is of daar tegenover voldoende waarborgen staan.

5.3 Aftapdilemmas (of: de geheimhoudersgesprekkencasus)

De wijze waarop overheden het gebruik van de voor hen beschikbare gegevens inrichten leidt tot praktische problemen die binnen de huidige wette-

88. Martijn (2015).

89. Vgl. Berkhout en van Engers (2012); Martijn (2015).

lijke kaders niet goed oplosbaar lijken. Illustratief daarvoor zijn de gesprekken van degenen van wie de communicatie geheim moet blijven, de zogeheten geheimhouders zoals onder andere advocaten. In deze ‘geheimhoudersgesprekkencasus’ gaat het om het spanningsveld tussen enerzijds het belang van opsporingsinstanties en het openbaar ministerie om op grote schaal vertrouwelijke telecommunicatie te kunnen aftappen, en anderzijds het belang dat advocaten en andere geheimhouders hebben erop te kunnen vertrouwen dat hun communicatie niet wordt afgetapt en afgeluisterd. In het verlengde daarvan is er natuurlijk het belang van het openbaar ministerie dat stevast niet ontvankelijk wordt verklaard wanneer het strafdossier transcripts van geheimhoudersgesprekken bevat.⁹⁰

Een praktisch probleem is dan het volgende. Voor geheimhoudersgesprekken is het zaak dat deze, in het geval van een overigens rechtmatige ‘tap’, worden weggefilterd, althans meteen worden verwijderd nadat deze zijn opgenomen. Maar om dat te kunnen doen moet uiteraard bekend zijn dat er inderdaad sprake is van zo een geheimhoudersgesprek. En om dat te weten te komen, moet ofwel het gesprek inhoudelijk worden verwerkt ofwel moeten de door advocaten gebruikte telefoonnummers bekend zijn gemaakt aan het openbaar ministerie. In Nederland is enkele jaren geleden voor de laatste oplossing gekozen.⁹¹

Risico XVI. Een fundamenteel risico is dan dat er een ontwikkeling is ingezet waarin degenen die aanspraak maken op geheimhouding of, in meer algemene zin bescherming van persoonlijke levenssfeer, dat alleen kunnen krijgen als zij zich als zodanig bekend willen maken.

En juist door die bekendmaking is er, zo wordt wel gevreesd, weer een risico dat aan die aanspraak voorbij wordt gegaan. Zo kan nu, omdat de geheimhoudingsnummers bekend zijn, onderzoek worden gedaan naar gebruiksprofielen van de betreffende dataretentiegegevens, iets wat voorheen voor het OM onmogelijk was. Ook wordt gericht af luisteren door de veiligheidsdiensten vergemakkelijkt. Dat deze vrees geen paranoïde fantasie hoeft te zijn blijkt uit enkele zaken die recent aan het licht kwamen.⁹²

90. Rb Amsterdam 20 december 2007 ECLI:NL:RBAMS:2007:BC0685 <http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2007:BC0685>.

91. College van Afgevaardigden van de Nederlandse Orde van Advocaten, Verordening van 1 april 2011, *Stcrt.* 2011, 6728. (Verordening op de nummerherkenning).

92. Zie brief van Pestman aan Plasterk d.d. 8 april 2014 (kenm. Prakken D'Oliveira/AIVD) te vinden via: [www.prakkendoliveira.nl/user/file/140408_-_kantoorklacht_aivd_\(mp_-_prakken_doliveira\).pdf](http://www.prakkendoliveira.nl/user/file/140408_-_kantoorklacht_aivd_(mp_-_prakken_doliveira).pdf) (geraadpleegd 1 januari 2016). En vervolgens: Vzr. Rechtbank Den Haag 1 juli 2015, ECLI:NL:RBDHA:2015:7436 te vinden via <http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2015:7436> (geraadpleegd 1 januari 2016) en daarover o.a.: AIVD ging te ver in af luisteren advocaten' NRC 19 december 2014); 'AIVD luistert advocaten al jaren af' De Volkskrant 19 december 2014; 'Advocaten dagen staat om af luisterpraktijken AIVD' NRC 22 april 2014.

5.4 Samenvatting

De transitie naar gedigitaliseerd bestuur (en naar de homo digitalis) leidt ertoe dat naarmate transacties tussen overheid, ondernemers en burgers worden gedigitaliseerd de hoeveelheid digitaal beschikbare data in omvang zozeer toeneemt dat er wel van Big Data wordt gesproken. Zonder daaraan te willen meedoen kan toch worden vastgesteld dat de overheid als geheel gaat beschikken over steeds dekkender informatiesystemen die (gedrag van) burgers en ondernemers beschrijven. En dat de mogelijkheid bestaat om al die informatie te koppelen en te analyseren.

We vatten weer samen op basis van de gesignaleerde risico's.

Risico XI. *Weinig wettelijke beperkingen.* Als het gaat om gegevensgebruik door en binnen de overheid is de wetgever maar in beperkte mate geneigd te voorzien in beperkingen met betrekking tot gegevensuitwisseling en gegevensanalyse.

Risico XII. *Wetgever laat bestuur te vrij.* Als het gaat om gegevensgebruik door en binnen de overheid is de wetgever maar in beperkte mate geneigd rekening te houden met beperkingen verband houdend met fundamentele rechten en vrijheden, zoals die waarin het Europees Handvest voorziet.

Risico XIII. *Kwetsbare wetgeving.* De wetgeving waarin te weinig rekening wordt gehouden met de bescherming van fundamentele rechten en vrijheden loopt het risico buitenwerking te worden gesteld. Voor de op basis daarvan gebouwde gegevensuitwisselingssystemen is dit een potentiële faalfactor.

Risico XIV. *Sleepnetpraktijken.* Digitale bestuurders hechten weinig betekenis aan beginsselen als select-before-you-collect en hebben weinig moeite met sleepnet-acties, als die effectief lijken om de door hen gestelde doelen te bereiken.

Risico XV. *Waarborgenerosie.* Er komen heel veel meer gegevens beschikbaar die door digitale overheden kunnen worden gebruikt, en waarschijnlijk ook gaan worden gebruikt, om macht uit te oefenen over burgers en ondernemers (offline, online en digitaal), zonder dat duidelijk is of daar tegenover voldoende waarborgen staan.

Risico XVI. *Databeschermingparadox.* Een fundamenteel risico is dan dat er een ontwikkeling is ingezet waarin degenen die aanspraak maken op geheimhouding of, in meer algemene zin bescherming van persoonlijke levenssfeer, dat alleen kunnen krijgen als zij zich als zodanig bekend willen maken.

We vrezen dat op het moment met de digitalisering bij de overheid een *Quod Licet Jovi* cultuur opbloeit – d.w.z. een cultuur van de dubbele standaard, waarin de overheid zich niet aan de regels hoeft te houden die voor de anderen gelden. Dan gaat het om het zich niet of *contre coeur* storen aan informatiebeperkingen die beogen de burger en de ondernemer te beschermen. Onze vrees berust op het kennelijke appèl dat uitgaat van een logica

als gehanteerd door Fred Teeven bij de bonnetjesaffaire: “ ... *Met de deal was overigens niets mis. Ook dat is gebeurd voor volk en vaderland ...* ”⁹³

Deel III. BESCHOUWING

6. Evenwichtige informatieverhoudingen

6.1 Op zoek naar tegenwicht

Het gaat in deze bijdrage over digitalisering en de vraag wat dat betekent voor de verhoudingen van burgers en overheden. We hebben in de voorgaande drie hoofdstukken van dit preadvies een groot aantal risico's in kaart willen brengen en bespreken in dit hoofdstuk welke positiefrechtelijke middelen het bestuursrecht te bieden heeft om aan enkele ervan het hoofd te bieden, en of daaraan iets hapert. We vatten dit ruim op. We gaan het dus hebben over burgers en andere bestuurden (organisaties, ondernemingen etc.) die als gevolg van digitalisering een andere positie krijgen c.q. innemen ten opzichte van de gedigitaliseerde overheid. Ons uitgangspunt is daarbij dat het een taak van het bestuursrecht is om eraan bij te dragen dat die verhoudingen zich ook in tijden van digitalisering evenwichtig ontwikkelen, dat wil zeggen: op een wijze die past binnen de grenzen die worden gesteld door grondrechten en beginselen van behoorlijk bestuur.

In reactie op de door digitalisering versterkte informatiepositie van de overheid wordt in de visiebrief van Plasterk gepleit voor het versterken van de informatiepositie van de burger.⁹⁴ Vanuit de gedachte van machtsverhoudingen is dat goed te volgen. De wijze waarop dit in de brief wordt ingevuld stelt evenwel, gelet op de mate waarin de informatiepositie van de overheid wordt versterkt, teleur. In de brief wordt ervoor gepleit dat burgers eenvoudig moeten kunnen zien welke gegevens over hen bij de overheid zijn vastgelegd en aan wie deze worden verstrekt. Verder moeten zij de mogelijkheid hebben om fouten te corrigeren. En dat moet worden gerealiseerd door burgers via MijnOverheid inzage te geven in de kerngegevens die overheden over hen vastleggen, met de mogelijkheid om online correcties door te geven. Er wordt aldus invulling gegeven aan het inzage- en correctierecht uit de Wet bescherming persoonsgegevens.⁹⁵

Waarom is dit teleurstellend? Omdat het versterken van de informatiepositie van burgers en het bewaken van evenwichtige informatieverhoudingen in een tijd van digitalisering naar ons gevoel meer omvat dan het

93. Aldus redeneert de aftredende staatssecretaris nog op de persconferentie van 9 maart 2015.

94. *Kamerstukken II* 2012/13, 26643, nr. 280, p. 5.

95. Art. 35 en 36 Wbp.

invulling geven aan inzage- en verbeteringsrechten waarover burgers allang beschikken. Het gaat erom dat we informatieposities en -verhoudingen van burgers tegenover de overheid zinvol kunnen duiden in een bestuursrechtelijke context, met bijbehorende effectieve rechtsbescherming.

In onze rechtssystemen zijn die machtsevenwichten min of meer organisch gegroeid aan de hand van de verschillende verhaallijnen die zijn ingezet door onder andere Hobbes, Locke, Montesquieu en Rousseau. De machtsevenwichten hebben zich natuurlijk doorontwikkeld, ook onder invloed van niet-juridische, vooral natuurwetenschappelijke, biologisch-medische en economische – en laatstelijk misschien ook cultureel-religieuze verhalen. Een digitale overheid vraagt om de inpassing van een aanvullend verhaal over de betekenis van wijzigende informatieposities. Evenals onze opvattingen over grondrechten, individuele veiligheid en individuele vrijheid ontwikkelt het bestuursrecht zich. En dat kan, zoals alles, onder voldoende druk vloeibaar worden. Zijn er onder de risico's die we inventariseerden zorgenkinderen die bijdragen aan het opvoeren van die druk?

6.2 *Zorgenkinderen*

We vatten nog even samen wat we in het voorgaande hebben vastgesteld.

Risico's bij beschikbaarheid en bereikbaarheid

Risico I. Digibeten de dupe. Digitalisering met besparingsambities kan ertoe leiden dat een grote groep minder digivaardigen (offline burgers en ondernemers) *de facto* wordt uitgesloten

Risico II. Digitale dwangbuizen. Het risico is dat de toegang tot steeds essentiëler wordende diensten van de digitale overheid wordt beheerst door regelingen met maar weinig waarborgen voor de gebruikers van deze diensten (de burgers)

Risico III. Troebel in plaats van transparant. Een risico voor de homo digitalis is dat digitale overheden in hun verhouding met burgers en ondernemers zich weten te onttrekken aan checks and balances door selectief hen betreffende informatie in meer of mindere mate toegankelijk te maken.

De genoemde risico's spelen vooral doordat digitalisering en de kennis daarover niet resulteren in gradueel veranderende communicatieprocessen die we gemakkelijk kunnen leren kennen. Het gaat met horten en stoten en niet iedereen kan die bijbenen. Ook omdat digitalisering vormen van 'formulierdwang' met zich brengt die moet worden gehoorzaamd omdat anders de door de burger gezochte overheidsdienst buiten bereik blijft.

Welke bestuursrechtelijke rechtsbescherming geniet een minder digivaardige homo digitalis, wanneer zijn gemeente besluit alles digitaal af te handelen en om het gemeentehuis alleen nog op donderdagmiddag open te stellen voor publiek? Welke bestuursrechtelijke rechtsbescherming geniet

een burger of ondernemer tegen de vormgeving van digitale formulieren die – direct in strijd met de beginselen van behoorlijk bestuur – onnodige verplichtingen op onvoldoende transparante motieven opleggen? Welke rechtsbescherming en rechtsmiddelen hebben we als het gaat om de vormgeving van die formulieren? Moeten we voor deze dingen naar de Ombudsman?

Kortom: is het bestuursrecht voldoende toegesneden op de strubbelingen die de vergrote inzet van informatietechnieken in termen beschikbaarheid en bereikbaarheid met zich mee kan brengen? We menen van niet. Traditionele bezwaarschiffenprocedures lijken, metaforisch gesproken, op kanonnen gericht op muggen, terwijl het ongemoeid laten van de muggen een malaria-epidemie zou kunnen veroorzaken.

Risico's met informatieveiligheid

Risico IV. Professioneel bestuur op basis van onwetendheid. Het bestuur weet niet goed wat informatieveiligheid is, wat het maatschappelijk en economisch belang ervan kan zijn en waar de verantwoordelijkheden liggen als het echt mis gaat.

Risico V. Complexiteit van materie. Voor bestuurders is de materie (veel te?) ontoegankelijk en bewerkelijk

Risico VI. Bestuurlijke aansprakelijkheid glipt weg. De politieke en bestuursrechtelijke aansprakelijkheid rond informatiebeveiliging en eID is niet eenvoudig te realiseren

Risico VII. Bestuurlijke zorgvuldigheid post hoc. De bestuursrechtelijke zorgvuldigheid bij (naar achteraf blijkt) relevante besluiten kon niet (of nauwelijks) ter discussie worden gesteld op het geëigende moment.

Risico VIII. Exoneratievergiert. De civielrechtelijke risico's rond informatiebeveiliging kunnen vergaand worden geminimaliseerd via exoneratieclausules

Risico IX. Beheervaardigheid is informatiefiltering. Het voor een verantwoord gebruik van de digitale overheidsdienstverlening vereiste niveau van digitale beheervaardigheden wordt de facto niet gehaald, en kan ook niet worden geëist van de offline en online burger (wel van de online en digitale bestuurder?), omdat dat in strijd wordt geacht met verworven informatievrijheden.

Risico X. Informatievrijheid impliceert botnets. Dit impliceert een risico voor hacking en botnets en daarmee ook voor de informatieveiligheid van communicatie tussen burgers en overheden en tussen overheden onderling.

Genoemde risico's spelen vooral omdat het bewaken van informatieveiligheid en van een veilige digitale identificatie-infrastructuur veel kennis vraagt uit uiteenlopende, zich nog sterk ontwikkelende gebieden (bijv. informatica, organisatiekunde).

Wanneer we de Diginotar-kwestie of het DigiD-drama als casus nemen (en afzien van beschouwingen over politieke verantwoordelijkheid) gaat het er niet alleen om hoe een burger of ondernemer beschermd wordt tegen de nadelige gevolgen van bestuurlijk onzorgvuldig digitaal handelen, maar

ook om hoe het bestuur, burger en ondernemer worden beschermd tegen hacking door kwaadwillenden en criminelen. Deze vormen van rechtsbescherming zijn problematisch – ook omdat de technologisch-organisatorische complicaties omvangrijk zijn en meestal verhinderen dat causaliteit gemakkelijk aannemelijk kan worden gemaakt. Wie het slachtoffer is geworden van identiteitsfraude als gevolg van het DigiD-drama zal die oorzaak niet of moeilijk voldoende aannemelijk kunnen maken. Wie de oorzaak van veiligheidsfalen is of was zal zich daarvan doorgaans uit onwetendheid niet eens bewust zijn.

De vraag is dan, kortom, of het bestuursrecht voldoende is toegesneden op de strubbelingen die de vergrote inzet van informatietechnieken in termen van informatieveiligheid met zich mee kan brengen. We menen opnieuw van niet. Het lijkt te gaan om vragen die betrekking hebben op de praktijk van behoorlijk besturen, maar hun invloed hebben buiten de context van de besluitvorming door bestuurders. Het gaat om vereiste kennisniveaus. Een heikel onderwerp. We bespreken aanbevelingen hieromtrent in het laatste hoofdstuk.

Risico's van overheidsgegevensgebruik

Risico XI. Weinig wettelijke beperkingen. Als het gaat om gegevensgebruik door en binnen de overheid is de wetgever maar in beperkte mate geneigd te voorzien in beperkingen met betrekking tot gegevensuitwisseling en gegevensanalyse.

Risico XII. Wetgever laat bestuur te vrij. Als het gaat om gegevensgebruik door en binnen de overheid is de wetgever maar in beperkte mate geneigd rekening te houden met beperkingen verband houdend met fundamentele rechten en vrijheden, zoals die waarin het Europees Handvest voorziet.

Risico XIII. Kwetsbare wetgeving. De wetgeving waarin te weinig rekening wordt gehouden met de bescherming van fundamentele rechten en vrijheden loopt het risico buitenwerking te worden gesteld. Voor de op basis daarvan gebouwde gegevensuitwisselingssystemen is dit een potentiële faalfactor.

Risico XIV. Sleepnetpraktijken. Digitale bestuurders hechten weinig betekenis aan beginselen als select-before-you-collect en hebben weinig moeite met sleepnet-acties, als die effectief lijken om de door hen gestelde doelen te bereiken.

Risico XV. Waarborgenerosie. Er komen heel veel meer gegevens beschikbaar die door digitale overheden kunnen worden gebruikt, en waarschijnlijk ook gaan worden gebruikt, om macht uit te oefenen over burgers en ondernemers (offline, online en digitaal), zonder dat duidelijk is of daar tegenover voldoende waarborgen staan.

Risico XVI. Databeschermingsparadox. Een fundamenteel risico is dan dat er een ontwikkeling is ingezet waarin degenen die aanspraak maken op geheimhouding of, in meer algemene zin bescherming van persoonlijke levenssfeer, dat alleen kunnen krijgen als zij zich als zodanig bekend willen maken.

Genoemde risico's spelen vooral, menen we, omdat het bestuur een belangrijke rol speelt bij wetgeving en in beleidsvormende processen. Daarbij worden de mogelijkheden van digitalisering enerzijds ervaren als een kans om de doelmatigheid van het overheidshandelen te vergroten en besparingsambities te realiseren, en anderzijds als een mogelijkheid om de handhaving te verbeteren op basis van een verbeterde informatiepositie. Voeg daar bij dat bestuurders nogal eens ervan overtuigd zijn dat het directe belang van hun werk vanzelfsprekend van meer gewicht is dan het belang van grondrechtelijke bescherming, en we hebben door de digitalisering een zichzelf versterkend mechanisme. Als gezegd vrezen we dat op het moment bij de overheid een *quod licet jovi* cultuur (dubbele standaard)⁹⁶ opbloeit met de toegenomen handhavingsmogelijkheden op basis van digitalisering. Dan gaat het om het zich niet of *contre coeur* storen aan informatiebeperkingen die beogen de burger en de ondernemer te beschermen, hetgeen op de werkvloer van overheden al snel als hinderlijk wordt ervaren.

Wanneer we de in hoofdstuk 5 beschreven *geheimhoudnummerkwestie* als voorbeeld nemen, gaat het om de bescherming tegen af luisteren van gesprekken tussen advocaten en hun cliënten, een bescherming die kennelijk alleen kan worden gegarandeerd wanneer bekend wordt gemaakt van welke telefoons voor geheimhoudgesprekken gebruik wordt gemaakt. Een dergelijk arrangement werkt alléén als erop kan worden vertrouwd dat van die kennis, van het weten waar geheimhoudgesprekken worden gevoerd, geen misbruik wordt gemaakt, ook niet onder de logica dat dit 'voor volk en vaderland' gebeurt. Eén en ander schreeuwt om nog meer onafhankelijk toezicht, zoals ook blijkt uit de recente uitspraak van het Hof Den Haag over het niet zonder onafhankelijk toezicht door de AIVD af luisteren van een advocatenkantoor.⁹⁷

De vraag is dan, kortom, of het bestuursrecht voldoende is toegesneden op het stelsel van verlokkingen dat de vergrote inzet van informatietechnieken in termen van informatiegebruik door de overheid met zich mee brengt? We denken dat hier twee gezichtspunten kunnen worden verdeeld. Door een positiefrechtelijke bril komt het ons voor dat er voldoende bestuursrechtelijke regels zijn waaraan de burger en de ondernemer rechtsbescherming zouden kunnen ontleen wanneer de overheid in zijn gege-

96. Uit wikipedia: 'Quod licet Iovi non licet bovi' of 'Wat Jupiter is toegestaan, is het rund nog niet toegestaan' is een Latijns spreekwoord dat in feite zegt dat wat een als belangrijk aangemerkt persoon mag, niet zomaar ook iedereen toegestaan is < https://nl.wikipedia.org/wiki/Quod_licet_Iovi_non_licet_bovi > (geraadpleegd op 30 oktober 2015).

97. Hof Den Haag 27 oktober 2015, ECLI:NL:GHDHA:2015:2881.

vensgebruik over de juridische schreef gaat. Maar door een rechtsrealistische bril menen we toch vooral te zien dat de overheid zich aan het aanwennen is om beperkende regels in de wind te slaan en om de sporen daarvan aan het zicht te onttrekken. We zouden aanbevelingen hieromtrent in het laatste hoofdstuk wel willen bespreken, maar realiseren ons dat we daar in de context van dit preadvies nog niet heel ver mee komen.

Wat uit één en ander naar voren komt is de betekenis van de kwaliteit van iemands *informatiepositie* waar het gaat om het verwezenlijken van een *rechtspositie*. Dit verwondert helemaal niet, en is ook niet nieuw. Het verkeerd inlichten van de Kamer door een bewindspersoon is niet voor niets al twee eeuwen een politieke doodzonde. Wat nieuw is, is dat informatieposities veranderen onder de druk van de digitalisering. En dat die digitalisering zozeer om zich heen grijpt dat iedereen aan de gevolgen voor zijn rechtspositie aandacht zal moeten besteden. Die aandacht gaat wat ons betreft uit naar het bewerkstelligen van evenwichtige informatieverhoudingen. Of het scheppen van condities waarin sprake kan zijn van digitaal ondersteund *fair play*.

Eén en ander brengt ons tot een voorlopige conclusie: door het verwezenlijken van de geïnventariseerde risico's bestaat de niet te verwaarlozen kans dat de informatieverhoudingen tussen enerzijds overheid en anderzijds de burger en ondernemer uit evenwicht raken, dat wil zeggen dat die niet meer passen binnen de grenzen die worden gesteld door grondrechten en beginselen van behoorlijk bestuur. Deze conclusie staat op twee benen. Tegen de risico's voor de burger en de ondernemer op de gebieden van toegang en veiligheid bestaan eigenlijk geen toegesneden bestuursrechtelijke instrumenten. En tegen de risico's voor de burger en de ondernemer die voortvloeien uit informatiegebruik binnen en tussen overheden voorziet het bestuursrecht weliswaar wel in allerlei regels, maar blijkt in de praktijk een adequate handhaving problematisch.

Enkele oorzaken zijn bekend. Ten eerste (i) is er natuurlijk de enorme toename aan informatie, informatietransacties en –bewerkingen. Ten tweede (ii) is er de aanmerkelijke dynamiek in aangeboden ICT-functionaliteit: het is moeilijk, zo niet onmogelijk geworden om als individuele burger, bestuurder of ondernemer de ontwikkelingen voldoende bij te houden. Deze oorzaak valt nagenoeg samen met de toegenomen noodzaak om over specialistische kennis te beschikken voor wie individueel verantwoordelijk wil zijn voor zijn deelname aan de digitale samenleving. Ten derde (iii) zijn er bij bestuursdiensten te veel visioenen of veronderstellingen over efficiëntie en effectiviteit van bestuurstoezicht op basis van digitale informatieverzamelingen en is er te weinig bewustheid van mogelijke rampsce-nario's, zoals dat van het DigiD-drama, en van de beperkte beveiliging

tegen kwaadwillige DDOS-aanvallen waarvan er één nog recentelijk de uitbetaling van toeslagen door de belastingdienst langdurig vertraagde.⁹⁸

De vraag die voorligt is of, en zo ja, in hoeverre de algemene en universele maatschappelijke transitie van offline bestuurders, burgers en bedrijven naar digitale bestuurders, burgers en bedrijven risico's met zich meebrengen voor ons begrip (en voor de hanteerbaarheid en dus flexibiliteit) van de bestuursrechtelijke beginselen en de via het bestuursrecht (dat immers op die beginselen rust) te beschermen rechten van burgers en ondernemers.⁹⁹

7. Wat kunnen we ermee?

7.1 In grote lijnen

We hebben aangewezen waar het bestuursrechtelijke bouwwerk onder druk komt te staan wanneer de samenleving en de overheid digitaliseren. Wat naar voren komt is de betekenis van de kwaliteit van iemands informatiepositie wanneer het gaat om het verwezenlijken van zijn rechtspositie. Daarbij speelt een drietal categorieën van vragen, zijnde:

- vragen van institutionele aard (bestuursrechtelijke instrumenten lijken in sommige gevallen bijvoorbeeld ontoereikend);
- vragen van vereiste kennisniveaus (ook hier schieten traditionele rechtsmiddelen tekort, zo laat het zich aanzien);
- vragen van bestuursmorele aard (een bestuurlijke bedrijfscultuur die opgewassen is tegen de verlokkingen die de digitalisering met zich mee brengt).

Waar we mee te maken krijgen is dat complexiteit en kennisgebreken bestuursrechtelijk op een zorgvuldige manier moeten kunnen worden behandeld. We weten nog niet goed hoe, maar denken dat daaraan vanuit verschillende richtingen wel kan worden bijgedragen. Bijvoorbeeld door weldoordachte mechanismen te organiseren voor het inrichten van bestuurlijke taken, in gezamenlijkheid met ofwel specialistische overheidsdiensten ofwel gespecialiseerde commerciële diensten. En bovendien door het inrichten van weldoordachte kaderscheppende mechanismen voor het outsourcen van publieke dienstverlening, maar dan zonder het politiek en

98. We doelen op de storing van 20 november 2015 bij banken en belastingdienst, waardoor mogelijk zo een 7 miljoen toeslagengerechtigden werden geraakt. Over de oorzaak ervan werd opmerkelijk zuinigjes gerapporteerd. Zie o.a. RTL-nieuws, 'Toeslagen later overgemaakt door storing Belastingdienst', 20 november 2015, te vinden via <http://www.rtlnieuws.nl/nieuws/binnenland/toeslagen-later-overgemaakt-door-storing-belastingdienst> (geraadpleegd 1 januari 2016).

99. Zie bijvoorbeeld Cliteur (2002).

bestuurlijk weglekken van verantwoordelijkheden. We zijn daar nog lang niet, zo blijkt uit de zorgwekkende afhankelijke positie die overheden innemen ten opzicht van bijvoorbeeld ondernemingen als Diginotar en Ordina of, als het gaat om van cybersecurity, van een specifieke dienstverlener als Fox IT.

We kunnen de rollen van de verantwoordelijke individuen onderscheiden in die van burger, ondernemer en bestuurder. We doen dit niet alleen omdat dit onderscheid in toenemende mate ook bij beleid en regelgeving van belang is geworden. Ook voor onze benadering, die ziet op bewust, verantwoord handelen is het van belang om te onderscheiden naar wat tegenwoordig wel *prikkels* worden genoemd, of in minder tegen de economische discipline aanhangende formulering: *motiveringstructuren*. Zonder terug te vallen op sociaalwetenschappelijke inzichten kunnen we hier uit de voeten met wat de rechtstraditie heeft opgeleverd. In grote lijnen draagt de individuele burger individueel de verantwoordelijkheid voor wat zij of hij doet, behalve wanneer zij of hij een onderneming met rechtspersoonlijkheid leidt of ervoor handelt (dan draait het bedrijf ervoor op) en behalve wanneer hij of zij als ambtenaar in functie handelt, in welk geval de overheid ervoor opdraait (met dien verstande dat wanneer het een politiek gevoelig mistasten betreft de ministeriële verantwoordelijkheid eveneens in werking kan worden gesteld.)

Wij menen dat het onderscheiden in burger-ondernemer-bestuurder van belang is omdat de onderlinge verschillen in motiveringstructuren aanzienlijk zijn, en hun rollen in termen van onder andere specialisatie en delegatie onontbeerlijk zijn in het steeds complexer wordende netwerk van interacties dat onze samenleving vormt en verwezenlijkt. En we menen ook dat we naast een consumentenrecht-achtige rechtsbescherming voor de homo digitalis ook een vorm van rechtsbescherming moeten kunnen bespreken waarin garanties te vinden zijn dat hij of zij zich op zijn eigen, individuele wijze kan blijven ontplooien en ontwikkelen.

7.2 Kritische aspecten

We hebben in het voorgaande 16 risico's gevonden waarmee de homo digitalis te maken krijgt. We hebben een aantal mogelijke oorzaken genoemd en in grote lijnen een drietal vraagstukken voor het bestuursrecht en bestuurspraktijk benoemd. En we hebben daarbij aangegeven dat de institutionele inrichting en vertegenwoordigingsarrangementen daarbij een rol spelen.

Wanneer we het in grote lijnen hebben over bestuursrechtelijke rechtsbescherming denken we, als gezegd, aan het legaliteitsbeginsel, de beginselen van behoorlijk bestuur en grondrechten als kaderscheppend. Kunnen we al die resultaten en overwegingen die we in de vorige paragraaf opsom-

den in verband brengen met de functionaliteiten van één en ander? Om dat overzichtelijk te houden benoemen we eerst een vijftal kritische aspecten.

Als eerste is van belang zich te realiseren dat er met de toenemende digitalisering vanuit het gezichtspunt van de verantwoordelijke individu een dynamiek ontstaat in wat hij of zij ervaart als eigen bevoegdheid en opgedrongen verplichtingen. Heel vaak worden efficiency, doeltreffendheid en controleerbaarheid als belangen in stelling gebracht. En heel vaak gaat dat ten koste van de discretionaire ruimte (autonomie, vrijheid). Een standaardvoorbeeld in dit verband is de lijst van zogeheten diagnose-behandel-combinaties, waaraan de vergoeding van het werk van een huisarts is gekoppeld en waardoor de huisarts die betaald wil worden blind moet zijn voor diagnoses die zijn kennis en ervaring hem voorhouden maar die in die lijst niet voorkomen – en zich dan ofwel bij de beperkingen neerlegt, ofwel in de verleiding komen kan om administratieve kunstgrepen te gaan toepassen die als valsheid in geschrifte kunnen worden geïnterpreteerd. Wij hebben in dezen geen oordeel over de verhouding autonomie-veiligheid bij digitale dienstverlening. We wijzen erop dat het gaat om een culturele kwestie die kan veranderen, en die vloeibaar lijkt te kunnen worden onder druk.

Over *evenwichtige informatieverhoudingen* als kritisch aspect hebben we het meeste wel gezegd in de vorige hoofdstukken. We merken alleen hier nog op dat het gaat om iets dat wel kan worden begrepen wanneer het wordt getoond, maar moeilijk kan worden gedefinieerd. Het zou goed zijn, denken we, wanneer daartoe door de wetgever een poging zou worden gedaan. Het hele begrip verdient hoe dan ook meer aandacht. We leven inmiddels in een wereld waarin de belangrijkste grondstof niet meer olie, maar informatie is.

Over *kennisvereisten* als broodnodige context voor *bestuurlijke zorgvuldigheid in digitale zaken* spraken we reeds. Maar ook over de omstandigheid dat de digitale wereld steeds ingewikkelder en complexer wordt en bovendien snel verandert. Het is onzeker in hoeverre van een individu (bestuurder, burger of ondernemer) kan worden verwacht van de meeste digitale zaken voldoende op de hoogte te zijn. Hier openbaart zich de noodzaak van samenwerking, institutionalisering en/of uitbesteding c.q. outsourcing naar specialisten.

Een daarmee samenhangend kritisch aspect is dan *de institutionele inbedding*. Economen hebben laten zien dat een rationale benadering mogelijk is. Oneerbiedig samengevat leiden hun (in respectievelijk 1991 en 2005 Nobelprijswaardig geoordeelde) bevindingen¹⁰⁰ tot de volgende heuristieken: (a) organisaties ontstaan voor wat een organisatie (institutie) efficiënter kan doen dan de markt, (b) eenmaal bestaande organisaties besteden iets dat ze nodig hebben uit aan een andere organisatie als daar

100. Coase (1937); Williamson (2005).

een markt voor bestaat en als een uitbestedingsovereenkomst geloofwaardig juridisch kan worden gehandhaafd. Die heuristieken lijken *mutatis mutandis* zo gek nog niet wanneer wordt nagedacht over institutionele veranderingen – bijvoorbeeld in het spoor van de Kaderwet zelfstandige bestuursorganen,¹⁰¹ die expliciet werd opgesteld voor het kunnen inrichten van onafhankelijke instituties die over specialistische kennis beschikken¹⁰² en voor het kunnen inrichten van bijzondere bestuursdiensten onder de hoede van een of enkele ministeries (we denken aan figuren die tot de inrichting van overheidsinstituties als het CIOT, ICTU en Luris hebben geleid). Trouwens, de ervaringen met die instituties laten zien hoe moeilijk het is om over de departementale grenzen heen werkelijk effectieve samenwerkingsverbanden te realiseren. Kennisdeling, kenniscapaciteit, outsourcing en specialisatie zijn elementen van een belangrijk organisatorisch kernaspect van onze bestuurspraktijk zolang die in transitie is door de digitalisering. Samenwerking over de soms nog parochiaal bewaakte departementale grenzen heen blijkt bovendien extra lastig.

Een ander belangrijk kernaspect van de transitie naar digitalisering betreft de steeds weer opduikende ambities en verwachtingen rond de volledigheid en toekomstbestendigheid van onze inzichten en daarmee samenhangende maakbaarheden van onderdelen van onze samenleving. Heel vaak wordt dan gedacht in de lijnen van wat we hier *de juridische Nirvana fallacy* noemen,¹⁰³ bijvoorbeeld wanneer wordt aangenomen dat maatschappelijke problemen door regelgeving kunnen worden opgelost of weggenomen. Dat dit in de praktijk maar zelden opgaat valt om ons heen waar te nemen. En daarvoor is een bijzondere reden wanneer we kijken naar digitaliseringsprocessen. Die houden altijd in dat er netwerken ontstaan. En dat leidt vooral tot complicaties wanneer de knooppunten in zo'n netwerk zich in verschillende tempi ontwikkelen.

Alles kent zijn tijd. Het gaat om het verwezenlijken van technologische innovatie, de behandeling van een rechtsgeschil, het aanpassen van beleid, van de wet, een cultuuromslag, etc. Dat allemaal loopt niet zonder meer synchroon. En toch hebben al de genoemde processen invloed op elkaar, als ze deel uitmaken van zo'n netwerk.¹⁰⁴

101. Stb. 2006, 587.

102. *Kamerstukken II* 2005/06, 27426, nr. 3.

103. In navolging van Demsetz (1969):1.

104. Een beroemd voorbeeld is de mededingingszaak in de Verenigde Staten die in de jaren 1960 door CDC tegen IBM werd aangespannen en die ging over de beschikbaarstelling van de interface-protocollen voor randapparatuur, zie bijvoorbeeld: Baase (1974). Deze zaak werd na 12 jaar procederen geschikt, op een moment dat er technisch inmiddels heel andere dingen speelden. Voor zover wij kunnen overzien heeft dit voorbeeld zich decennia later in Europa opnieuw voorgedaan in de Microsoft-zaak (Page and Lopatka (2009)). Dit soort complexiteit blijkt lijkt veel hardnekkige politiek-juridische vraagstukken te kenmerken (privacy, ICT-aanbestedingen, duurzaamheid, vluchtelingen). Maakbaarheid en voorspelbaarheid blijken beperkt (zie ook Appendix 3).

Er zijn dan dus vragen en onzekerheden over behoud van discretionaire bevoegdheden van gebruikers, over motiveringstructuren en effectieve institutionele inbedding, en over het tegengaan van de juridische *Nirvana fallacy*. Eén en ander leidt tot het vermoeden dat we niet al te veel moeten hopen op een enkele bestuursrechtelijke ‘*silver bullet*’ waarmee we de problemen snel en effectief uit de wereld kunnen helpen.

Maar dat is niet alles. Er zijn ook meer positieve ‘bottom-up’ ontwikkelingen. Ze rusten óók op de mogelijkheden van de digitalisering (denk aan de manier waarop de inhoud van Wikipedia op basis van enkele regels en afspraken door de gebruikers zelf wordt bewaakt op kwaliteit, en tegen kwaadwillige aanvallen¹⁰⁵) die zouden kunnen bijdragen aan verbetering van de hanteerbaarheid van de complexiteit. Omdat we menen dat het van betekenis is om daarop te anticiperen bespreken we een mogelijke ontwikkeling hieronder aan de hand van een voorbeeld waarvan het maatschappelijk belang moeilijk kan worden overschat: de app-revolutie.

7.3 De app revolutie

We gaan op zoek naar een functionele ontwikkeling in de digitalisering die thans gaande is en waarschijnlijk van grote betekenis gaat worden om de gesignaleerde complexiteit te beteugelen, dat eigenlijk al is en doet, maar die daarbij tegelijkertijd weer nieuwe risico’s voor onevenwichtige informatieverhoudingen met zich brengt. We gebruiken die ontwikkeling als demonstratiemateriaal. We kiezen de *app*-ontwikkeling en geven aan waarom die van zo grote betekenis is voor de verschijningsvormen van de digitale wereld.

Proprietary én open source bedrijfsmodellen voor smartphones: institutionele inbedding (i)

In 2007 kwam de eerste iPhone op de markt die werkte op iOS (het *proprietary* smartphone platform van Apple); in 2008 de eerste HTC die werkte onder Android (het *open source* smartphone platform dat Google haast onmiddellijk als tegenhanger van iOS beschikbaar stelde).

Zowel iOS als Android bieden ‘toolkits’ die het vervaardigen van apps ondersteunen en standaardiseren. Beide bieden een distributie-en-betalpad. En beide bieden een zekere mate van toezicht op kwaliteit. Vooral het kwaliteitstoezicht én het bedrijfsmodel verschillen: iOS Apps moeten door Apple worden getoetst en gedistribueerd, en een aanmerkelijk percentage van de opbrengst moet aan Apple worden afgedragen. Vergelijkbare inmenging van Android is aanmerkelijk minder of afwezig. Wat opmerke-

105. Zie bijvoorbeeld Heaberlin en DeDeo (2015). Hun aanpak wordt nader geplaatst in Appendix 3.

lijk genoemd kan worden is dat de twee platforms iOS en Android, die naar hun bedrijfsmodel zo verschillen, naar functionaliteit haast niet van elkaar verschillen, althans niet voor de meeste gebruikers c.q. consumenten.

Ontwikkeling van Apps vanaf 2007 tot heden

Vanaf 2007, toen de markt voor apps ontstond, is deze stormachtig gegroeid. Medio 2015 wordt gerapporteerd dat in de voorafgaande 12 maanden 25 miljard iOS apps werden gedownload, en 50 miljard apps voor Android.¹⁰⁶ Dat is samen 75 miljard(!) In 2014-2015 werden (op een wereldbevolking van 7.3 miljard) iets meer dan 10 apps per wereldburger gedownload. De platforms iOS en Android, die medio 2014 respectievelijk zeven en zes jaar bestonden, hebben dus een explosieve groei doorgemaakt en voor een explosieve groei gezorgd. We hoeven dan ook niet meer aan juristen uit te leggen wat smartphones en apps zijn. Er zijn, vermoeden wij, maar weinig juristen in Nederland die geen gebruik maken van tenminste één smartphone en een tiental apps of meer.

Smartphones als voorbeeld van Internet of Things: institutionele inbedding (ii)

Apps leveren diensten die zo kunnen zijn ingericht, dat ze samenwerken met andere apps en/of toegang nodig hebben tot informatie van elders ('the cloud') en dat voor die samenwerkingsmogelijkheden meestal keurig netjes toestemming wordt gevraagd en verkregen.¹⁰⁷ Dit in overeenstemming met de wettelijke regelingen die de persoonlijke levenssfeer beogen te beschermen.

Maar omdat het verlenen van toestemming is gerelateerd aan het verwerven van functionaliteit wordt die toestemming doorgaans vrij gemakkelijk verleend en verkregen. Veel apps vragen en krijgen toestemming om toegang tot foto's, netwerkfuncties, adressen, locatiegegevens. Eigenlijk weet niemand op dit moment het antwoord op twee belangrijke vragen: (1) wat mogen de app-aanbieders die toestemming kregen met de verkregen gegevens doen en wat niet, en (2) wat doen die app-aanbieders er in feite mee. Het is meer dan aannemelijk dat rechtmatig verkregen (persoons) gegevens worden doorverkocht of -geleverd (doorgaans als voedsel voor de voor consumenten weinig transparante geautomatiseerde carrousels met veilingen van profielinformatie, of als voedsel voor de ook proactief georiënteerde analyses van politie- en veiligheidsdiensten). En daarmee, dat de

106. Google Play downloads reached 50 billion in the last 12 months, while Apple's app store downloads totaled 25 billion. Amy Gesenhues on June 16, 2015 at 1:12 pm at: <http://marketingland.com/google-play-gaining-ground-against-apple-as-android-app-downloads-outnumber-ios-2-to-1-132307>.

107. Dit geldt inmiddels ook voor Android apps, tenminste vanaf versie 6.0 [Lollipop].

wereld van de smartphones een belangrijk voorbeeld is geworden van wat het ‘Internet of Things’ of ‘IoT’¹⁰⁸ wordt genoemd.

De ‘use-case’ dimensie

Apps zijn dan, als onderdeel van dat IoT, als knooppuntjes in een wereldwijd netwerk, een emergent verschijnsel. Het succes is vermoedelijk mede ingegeven door de omstandigheid dat toepassingen in de vorm van apps aan beperkingen onderhevig zijn. Want smartphones hebben – hoewel deze *devices* qua architectuur volwassen computers zijn – beperkte mogelijkheden (batterij, schermgrootte, processor, geheugen e.d.), evenals smartphonegebruikers te maken hebben met beperkingen (tijd, aandacht, ICT-kennis, soorten digitale behoeften etc.). Door die wederzijdse beperkingen op elkaar af te stemmen is een nieuw standaardformaat voor programma’s (*applications* d.w.z. ‘apps’) op mobiele apparatuur ontstaan dat buitengewoon effectief en succesvol is. Zo succesvol, dat ze onderweg zijn een nieuwe *de facto* standaard te worden voor digitale diensten.

Apps zijn doorgaans programma’s met een beperkte functionaliteit, je kunt ze niet voor alles gebruiken, maar wel voor een zogeheten *use case*, dat wil zeggen: voor een dienst met de dimensie van de een of andere standaardtaak, van iets wat de gebruiker goed kent en vaak doet en waarvoor je een digitaal steuntje in de rug kunt gebruiken. Voor wanneer je wilt weten wat voor weer het is in Den Haag, als je een SMS wilt lezen, een tweet wilt twitteren, wanneer je wilt weten of je nog een mailtje hebt gekregen, of voor het bekijken van je banksaldo, of de digitale post van de belastingdienst.

Het gebruik van dat soort dienstjes is vaak heel intuïtief. Er zijn meer dan een anderhalf miljoen verschillende apps beschikbaar voor Android en vermoedelijk meer dan half zoveel voor iOS. Vaak hebben ze via internet toegang tot de servers en databases van een ‘back office.’ De wereld van computergebruikers is razendsnel aan het veranderen in de richting van een wereld van app-gebruikers.

Standaard objectarchitectuur

De term ‘use case’ laat zich niet gemakkelijk vertalen en is afkomstig uit het domein van de informatica in de jaren 1980, toen er een beweging opkwam onder informatici om programmatuur zo te gaan inrichten dat bouwstenen hergebruikt konden worden. Die bouwstenen werden ‘objecten.’ En de standaardarchitectuur van objecten bestaat uit een compartiment voor data en voor functionaliteit (‘methods’) en voor input en output (‘message’). Object oriëntatie werd een doorslaand succes, mede doordat in de afgelopen twintig jaar omvangrijke bibliotheken met objecten (en dus: methods) beschikbaar kwamen en omdat computertalen als Java

108. Morgan (2014).

gericht werden op het bouwen en integreren van objecten. Zowel iOS (met objective C) als Android (met Java) ondersteunen het programmeren van objecten.

Samengevat komt de apps-explosie van 2015 met kansen en met bedreigingen. De kansen worden geboden door de ‘use-case’ dimensie van apps, die er tezamen met de standaard objectarchitectuur toe lijkt te leiden dat de digitalisering voor consumenten, bedrijven en dienstaanbieders aanmerkelijk transparanter kunnen worden dan ze tot nu toe waren, tenminste, wanneer er standaarden ontstaan voor functies waarvoor toestemming nodig is en voor de protocols waarvan dat soort functies gebruik maken om te communiceren. De bedreigingen bestaan in de kans dat die standaarden *niet* ontstaan en *niet* worden omhelsd, en dat de apps wereld verder tot een volkomen ondoorzichtige en onveilige kluwen van onderling verbonden diensten (en via die diensten verbonden belangen) zal uitgroeien.

Belangrijke vragen gaan dan natuurlijk in de toekomst ook (en nog steeds) over evenwichtige informatieverhoudingen tussen app gebruikers en app aanbieders. En dat evenwicht berust op het effectief kunnen authentifieren van gebruikers, aanbieders en apps, het hebben van toegang, het bestaan van transparantie en van betrouwbare, integere communicatie. We menen dat zulks alleen mogelijk is op basis van effectieve standaarden en *protocols*. En we menen dat het bestuursrecht hier een rol heeft te spelen, al was het alleen maar om bestuurlijke taakvervulling digitaal te kunnen uitvoeren op een digitale wijze die tegelijkertijd recht doet aan elementaire beginselen van bestuurlijk behoren.

7.4 Apps van de overheid

De digitale overheid gaat zelf natuurlijk ook apps aanbieden om haar dienstverlening voor burgers (gebruikers) beschikbaar te maken. De overheid kan daarbij, eventueel zelfs zonder dat voor te leggen aan wetgever of belanghebbende, informatiefunctionaliteiten inbouwen, zonder om toestemming te vragen, dat wil zeggen: de toegang tot de dienst te weigeren wanneer de toestemming niet wordt gegeven. Apps van overheden kunnen, doorgaans zonder democratische of bestuursrechtelijke toetsing, toegang tot informatiefunctionaliteit van burgers en ondernemers claimen. Alsdan kan een situatie ontstaan waarin de machtsverhoudingen tussen het bestuur (als app-aanbieder) en de burger of ondernemer (als app-gebruikers) uit evenwicht raken.

Hier komt opnieuw naar voren wat Locke en Montesquieu van belang oordeelden als randvoorwaarde voor het domesticeren van bestuursmacht: het primaat van de ‘liberty’ (we begrijpen *liberty* als samengesteld uit vrijheid en autonomie) boven ‘security’ (wat we begrijpen als samengesteld uit zekerheid en veiligheid). We kunnen ons niet aan de indruk onttrekken dat wat de digitalisering vooral met zich meebrengt een terugkeer is naar

het waarden van veiligheid boven *liberty*,¹⁰⁹ mogelijk doordat het doorzien en beïnvloeden van digitale diensten moeilijk is. En we vragen ons ook af of die omgekeerde tendens mede het gevolg is van de mate waarin onzekerheid in de samenleving toeneemt ten aanzien van terrorismedreigingen, maar ook ten aanzien van ondoorzichtige en nauwelijks door het recht betugelde digitalisering bij bedrijfsleven en bij de overheid, en misschien ook doordat de betreffende overheden er niet in lijken te slagen de burger ervan te overtuigen dat de problemen onder controle zijn. We vragen ons af of de app revolutie de mogelijkheid opent dat de burger hierbij de overheid te hulp schiet.

We herinneren ons nog levendig de tijd waarin heftig werd gedebatteerd over de wenselijkheid van het elektronische patiëntendossier (EDP). De discussie liep erop uit dat de Eerste Kamer het project zo goed als afblies. Ergens gedurende dat proces bood Google aan om een EDP als cloud-dienst aan te bieden. Daarop is niet ingegaan – vermoedelijk ook omdat er geen aanbesteding was waarop Google had ingeschreven en als winnaar te voorschijn was gekomen – maar ondenkbaar is het niet dat de overheid die immers baat heeft bij het zoveel mogelijk doen uitvoeren van de haar opgedragen taken op digitale wijze, er toe komt die taken via cloud-diensten te outsourcen als aan de daaraan te stellen eisen zou zijn voldaan.

In een app benadering zou dat EDP er als volgt kunnen uitzien: een EPD-app op je smartphone die het EDP van de eigenaar bevat als data en die via messages over het internet in verbinding staat met *devices* van de medici van dienst. In een app-benadering zou het systeem voor het niet-afluisteren van advocatengesprekken er eveneens anders kunnen uitzien: de betreffende app zou dan de afluisterdienst van het geheimhoudingskarakter van de voorliggende smartphone aan de afluisterdienst kunnen signaleren. Op die wijze zou in de app-benadering een belangrijk deel van het werk door de burger of ondernemer worden gedragen en beheerd op zijn smartphone.

Ook dan blijven de belangrijkste rechtsvragen nog onvoldoende beantwoord. Ze betreffen niet alleen het effectief authenticeren van gebruikers (burgers, ondernemers), aanbieders (overheden) en apps, en het garanderen van betrouwbare communicatie, maar ook het betrouwbaar monitoren en archiveren van digitale transacties ten behoeve van eventuele bewijs-

109. Dit lijkt te worden gekoesterd: in december 2015 kregen we een paniekbericht onder de vlag van NL-Alert op onze smartphone met de vraag of we de rampeninformatie-app wilden activeren – het was een proef, maar het weigeren van de dienst bleek een heel gedoe waarvan wij vermoeden dat menige offliner daarin niet zal zijn geslaagd. We vragen ons trouwens wel af of zo'n proef aan de eerste beginselen van het recht op een persoonlijke levenssfeer voldoet. Mag een overheid ongevraagd paniek zaaien om een overheids-app te testen? Het lijkt ons een illustratie van het toenemende belang dat de overheid ziet in zijn rol van beveiliging, ten koste van het belang van zijn rol als bewaker van onze autonomie/vrijheid.

voering achteraf. Die dingen zijn er nu, bij de bestaande ICT infrastructuur waarvan overheid, bedrijven en burgers gebruik maken, niet. Misschien kan dat bij een ICT-infrastructuur gebaseerd op apps wel, of beter. Dit (anno 2016) lijkt het jaar om dat uit te vinden. In de volgende paragraaf laten we daarom onze verbeelding spreken ten aanzien van de mogelijkheden van een gestandaardiseerde app-benadering voor overheden.

7.5 Waarheen?

Eerder concludeerden we dat door het verwezenlijken van de geïnventariseerde risico's de niet te verwaarlozen kans bestaat dat de informatieverhoudingen tussen overheid, burger en ondernemer uit evenwicht raken. Dat is betekenisvol omdat evenwichtigheid van informatieverhoudingen bijdraagt aan individuele vrijheid. Immers wanneer er een verschil van inzicht bestaat tussen een burger of bedrijf met de overheid over een overheidsbesluit of -regeling (of de manier waarop die wordt gehandhaafd) is het resultaat mede afhankelijk van de mate waarin de informatieposities van beide partijen in evenwicht zijn. Equality of digital arms is noodzakelijk voor het kunnen verdedigen, tegen de digitale overheid, van de individuele vrijheden van homo digitalis.

Maar wat moeten we daar nu mee? Een vraag die ons, bij wijze van gedachtenexperiment, relevant voorkomt is wat een burger, homo digitalis, kan doen als hij of zij meent dat de informatieverhouding met de overheid uit evenwicht is geraakt. Kan deze homo digitalis met enige kans op succes een beroep doen op een beginsel van behoorlijk bestuur? Kan een evenwichtige informatieverhouding worden geëist, bijvoorbeeld in het kader van het verbod op *détournement de pouvoir*? Zou zo een bijzondere interpretatie kunnen postvatten, bijvoorbeeld onder de noemer *détournement de pouvoir digitale* of *équilibre de relations digitale*?

Détournement de pouvoir digitale?

We zijn dan op zoek naar een uitwerking van het verbod van de *détournement de pouvoir* waarmee informatieverhoudingen in evenwicht kunnen worden gebracht. We denken dan bijvoorbeeld aan de daaraan verwante vereisten van doelbinding of doelverenigbaarheid en transparantie (resp. art. 9, eerste lid, Wbp en art. 33 en 34 Wbp). Die vereisten verlangen dat persoonsgegevens, die voor een bepaald doel zijn verzameld, niet mogen worden gebruikt voor een ander, daarmee onverenigbaar doel, alsmede dat de wijze waarop en het doel waarvoor persoonsgegevens worden gebruikt transparant wordt gemaakt. Voor wat we ermee willen bereiken zouden we dan kunnen denken aan de uitwerking dat de informatie verkregen in het kader van de éne publiekrechtelijke taak alléén mag worden gebruikt voor andere publiekrechtelijke taken, als er is voorzien in passende waarborgen en effectieve mogelijkheden van verantwoording van hoe de informatie is

gebruikt. Voor deze waarborgen kan dan aansluiting worden gezocht bij de voor het doelbindingsbeginsel ontwikkelde criteria. Verdergaande waarborgen zijn passend als gevolgen van het verdere gebruik van de gegevens voor de burger ernstiger kunnen zijn, als de gegevens niet rechtstreeks van de burger zijn verkregen, als de aard van de gegevens gevoelig is, als er minder verwantschap is tussen de verschillende publiekrechtelijke taken (vgl. art. 9, tweede lid, Wbp).¹¹⁰

We menen dat de huidige stand van de Nederlandse rechtsstaat in de praktijk nog ver verwijderd is van dit ideaalbeeld, en dat er weinig uitzicht is op spontaan herstel. We menen ook dat het de moeite waard zou zijn na te gaan of, wanneer de digitale overheid er toch toe overgaat zijn diensten in de vorm van apps aan te bieden, de bijbehorende standaarden en communicatieprotocollen niet zo kunnen worden ingericht dat de verzwakking van de informatiepositie van de burger tenminste voor een deel wordt hersteld, bijvoorbeeld door hem meer zeggenschap te geven en hem aldus mede-verantwoordelijk te maken voor het bewaren en beheeren van eigen persoonsgegevens.

Digitaal-materiële zorgvuldigheid?

Een andere vraag is of we, wanneer de overheidsdienst blijk geeft van te weinig kennis van informatica en/of organisatiekunde, een beroep kunnen doen op het vereiste van materiële zorgvuldigheid, d.w.z. het vereiste van art. 3:4, tweede lid, Awb. Op grond daarvan worden bestuursorganen geacht de rechtstreeks bij een besluit betrokken belangen af te wegen, voor zover niet uit een wettelijk voorschrift of uit de aard van de uit te oefenen bevoegdheid een beperking voortvloeit. Daarbij mogen de voor een of meer belanghebbenden nadelige gevolgen van zo een besluit niet onevenredig zijn in verhouding tot de met het besluit te dienen doelen.

We vragen ons, weer bij wijze van gedachtenexperiment, af hoe deze bepaling zou kunnen worden gelezen als het gaat om een Iraanse burger die ernstig is gedupeerd door het DigiD-drama en daarom rechtsmiddelen zou willen instellen tegen het ‘besluit’ van de minister om er in het kader van het DigiD-drama bij Microsoft op aan te dringen niet over te gaan tot het intrekken van valse certificaten? Is hij geen belanghebbende? Zijn bij de besluitvorming door de minister de belangen van Iraanse burgers afgewogen? Is er bewijsmateriaal? Hebben we een begin van een idee wat we bedoelen wanneer we het over digitaal-materiële zorgvuldigheid hebben?

110. Zie daarover bijv. Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 April 2013.

7.6 Een conclusie en enkele aanbevelingen

Wij denken dat dergelijke vragen, vragen naar concrete claims, naar interpretaties en naar rechtsontwikkeling van groot belang zijn. Maar we denken ook dat wij daarover op deze plaats, en op dit moment, nauwelijks iets met gezag kunnen zeggen omdat er, voorzover wij overzien, nog maar weinig gerichte klachten over de risico's die wij inventariseerden werden voorgelegd aan de rechter.

Ons algemene beeld is, dat het in veel individuele gevallen moeilijk zal zijn om handvaten te vinden die toereikend zijn voor de homo digitalis om zijn rechtspositie te verdedigen. We denken ook dat dit een cruciale uiting is van verstoorde en onevenwichtige informatieverhoudingen tussen burger en bestuurder. De voornaamste problemen hierbij zijn vermoedelijk direct terug te voeren op asymmetrische informatieposities. Dit geldt in elk geval wanneer onduidelijk is of een besluit is genomen, of een juiste belangenafweging heeft plaatsgevonden en of er bewijsmateriaal beschikbaar kan worden gemaakt. En die onduidelijkheden gelden voor veel van wat de *homo digitalis* kan overkomen als gevolg van overheidsdigitalisering.

Onze hoofdconclusie is dan ook onthutsend. Onze democratie en onze rechtspraak blijken, oog in oog met de huidige maatschappelijke transitie naar een digitale samenleving kwetsbaar voor belangrijke en mogelijk schadelijke bijeffecten zonder zich daarop effectief voor te bereiden. Hiermee raken we aan het eind van ons Latijn.

Wel hebben we nog enkele aanbevelingen die uit het voorafgaande volgen. Deze gaan erover hoe, als jurist, om te gaan met de voortschrijdende digitalisering van de wereld en het bestuur. Wij zien twee actielijnen, die geen van beide wetswijzigingen omvatten, wel beleidsaanpassingen.

1. Ad hoc rechtsontwikkeling op basis van feitelijke situaties die zijn ontstaan.

Het is van het grootste belang dat de rechter en de rechtspraak veel actiever worden ingezet om antwoorden te vinden op het beteugelen van de bestuursrechtelijke risico's die we inventariseerden en die de transitie naar een digitale samenleving met zich meebrengt. We leven in turbulente tijden, zowel juridisch als digitaal, waar de rechtsontwikkeling in belangrijke mate hangt op de rechtspraak, op individueel juridisch talent, oog in oog met een verrassende en aansprekende digitale casus die al dan niet toevallig een centraal probleem treft en via de rechtspraak tot een vruchtbare uitkomst leidt. We vermoeden dat de materiële bestuurlijke zorgvuldigheid wel wat opheldering *in digitalibus* kan gebruiken.

We vermoeden ook dat onder de huidige omstandigheden niet te veel van wetgeving hoeft worden verwacht omdat daarmee vaak doelen worden beoogd in een omgeving die waarschijnlijk al van kleur is verschoten nog

voordat tot handhaving kan worden overgegaan. Omdat zowel de techniek als de politieke verhoudingen inmiddels op hun eigen wijze en in hun eigen tempo blijken te zijn veranderd. Een schoolvoorbeeld lijkt de ontwikkeling van de wettelijke bescherming van de persoonlijke levenssfeer te bieden, tegen de achtergrond van de ontwikkelingen van economische en technologische bedrijfsmodellen die zijn gebaseerd op de verwerking van persoonsgebonden informatie.

We menen daarom dan ook dat het aanbeveling verdient te bevorderen dat de rechter vaker wordt ingezet door of namens de homo digitalis, wanneer die zich op digitale wijze buiten spel voelt gezet en aan den lijve de gevolgen ondervindt van het uit evenwicht raken van informatieverhoudingen.

2. Standaardisering van ICT op een wijze die tegemoet komt aan vereisten voor herstel van maatschappelijk vertrouwen in de digitale overheid.

Alle geïnventariseerde risico's kunnen eraan bijdragen dat een bestuurlijke praktijk ontstaat waarin wantrouwen en misverstand tussen burgers, ondernemers en bestuurders de overhand krijgen. Wij vermoeden dat we die route in de praktijk al aan het verkennen zijn wanneer we denken aan de mislukte ICT-projecten van de overheid, aan de verplichte digitalisering van communicatie tussen de burger (met inbegrip van de minder digivaardige offliner) en de belastingdienst, en aan de weinig bemoedigende handhavingstatistieken bij cybercriminaliteit.

Wanneer we in aanmerking nemen dat er zelfs onder de huidige, gebrekkige beveiligingsmogelijkheden een ontwikkeling gaande is naar een digitale overheid menen we dat daarmee de noodzaak is ontstaan om effectief te werken aan behoud (of herstel) van vertrouwen. Die noodzaak rust op het besef dat, wanneer alle risico's die we hebben geïnventariseerd *tegelijktijdig* zouden gaan spelen, de gevolgen onrustbarend, om niet te zeggen: ontwrichtend zouden zijn. We vermoeden dat hiermee een politieke noodzaak bestaat om tot een gelaagd fundament van betrouwbare infrastructuurele protocollen en diensten te geraken waarop de individuele transacties in vrijheid en veilig kunnen worden aangegaan. In elk geval, en tenminste, voor de transacties van en met overheden.

Het verdient daarom aanbeveling om deze weg serieus te onderzoeken, met name nu we de overgang naar bestuurlijke dienstverlening via apps meemaken, wat een waterscheiding zou kunnen markeren. Een waterscheiding die als het goed gaat de stroom in de richting stuurt van effectief authenticeren van gebruikers (burgers, ondernemers), aanbieders (overheden) en apps, van het garanderen van betrouwbare communicatie, en van het betrouwbaar monitoren en archiveren van digitale transacties door de overheid ten behoeve van eventuele verantwoording en bewijsvoering achteraf, maar die als het fout gaat de stroom ook een richting in kan sturen

van een digitale jungle, waarbij de wetten van de jungle de overhand krijgen.¹¹¹

Ten slotte

En voor wie nu, aan het einde van ons betoog, zich teleurgesteld realiseert dat we geen enkele positiefrechtelijke vraag concreet en gezaghebbend hebben beantwoord, geen enkele vraag die hij of zij in zijn of haar commerciële praktijk zou mogen hebben, resteert terugverwijzing naar onze aanbeveling om rechtsvragen *in digitalibus* aan de rechter voor te leggen. En daarbij nog een aansporing – wees vooral vasthoudend als een terriër, wanneer de ‘inequality of digital arms’ een omvang aanneemt die naar uw oordeel niet door de beugel van de bestuurlijke behoorlijkheid gaat.

APPENDICES

Appendix 1. Iets over de homo digitalis (of de menselijke natuur) als voorwerp van rechtswetenschappelijke overweging

In dit preadvies verdiepen wij ons in de rechtspositie van de *homo digitalis*, de mens die in een gedigitaliseerde wereld zijn weg moet vinden en zich moet zien te handhaven. Het is ons inziens noodzakelijk uiteen te zetten wat we verder bedoelen met de notie van *homo digitalis* (als bestuurder en als bestuurd). We ontlelen daarbij inzichten aan menstyperingen zoals die in andere disciplines wel een bijzondere rol spelen, zoals de *homo economicus*, de *homo ludens*, de *homo universalis*, de *homo sapiens*, etc. Deze bijlage heeft dan drie delen. In het eerste (*Welk beeld past bij het begrip homo digitalis?*) bezien we hoe het begrip *homo digitalis* thans wordt begrepen, op basis van het gebruik ervan op het internet. In het tweede (*Waarom een homo digitalis?*) gaan we op zoek naar een functie die het begrip deelt met zusterbegrippen (*economicus*, *ludens*, *sapiens*). In het derde gedeelte (*De homo digitalis als autonoom individu*) van deze bijlage geven we aan in welk opzicht de *homo digitalis* een bijzondere karakterisering van de mens als voorwerp van rechtswetenschappelijke studie is.

1. Welk beeld past bij het begrip homo digitalis?

Juristen zijn niet de eersten die aangetrokken bleken door de term *homo digitalis*. Antropologen, bijvoorbeeld, waren ons voor. We geven hier een

111. Om te voorkomen de indruk te wekken dat we zelf inmiddels ook slachtoffer zijn geworden van een Nirvana fantasie (die doorgaans resulteert in de Nirvana fallacy) hebben we enkele beschouwingen hierover opgenomen in Appendix 3.

paar citaten uit Antropologi.info,¹¹² een blog of webforum van antropologen:

*“How do people in Britain use the internet? How do they behave online? **The new Digital Anthropology Report.** The Six Tribes of Homo Digitalis gives some answers.*

*The British communication company Talk Talk sent researchers from the University of Kent into the homes of people around the UK to ask them questions about their attitudes towards digital technology and to watch them use it. They also commissioned anthropology professor **David Zeitlyn** to analyse the findings.*

They found that “homo digitalis” consists of Six Tribes with very different attitudes, usage patterns and modes of behaviour. Some of these tribes have embraced technology and put it at the centre of their lives. For other tribes, ‘the internet’ is a rather frightening jungle.

*The **E-ager Beavers** are the largest tribe by quite a distance, with 29% of the UK adult population. They use the internet heavily, but they are more passive users. They lack the confidence or the drive to get involved with uploading their own content or producing their own blogs.*

*The **Timid Technophobes** are the second largest group (23%). They have only limited internet skills and will only use it when they really need to. They still prefer to use pen and paper and prefer to send and receive letters. They don’t read blogs and are not interested in facebook either.*

*The tribe of the **Digital Extroverts** (9%) consists of people who are “always-on”. They are active bloggers, use twitter, flickr etc. “Regularly updating their online profile is as much a part of their daily routine as eating.” The ability to interconnect and share data is a prerequisite.*

According to Zeitlyn, your willingness to embrace technology and integrate it into your life will dictate your success in life far more than your social class will. As class structures change quickly, he writes in his analysis, the extent to which people use social networking and promote themselves online will become more important in determining their careers than what school or university they went to.”

Daaruit kan worden afgeleid dat het begrip homo digitalis in de sociale wetenschappen al wordt gebruikt als een overkoepelend begrip om, op basis van gedragskarakteristieken in relatie tot de digitalisering, groepen te kunnen onderscheiden en hun sociale betekenis te beoordelen.

112. <http://www.antropologi.info/blog/anthropology/2009/digital-anthropology-report>.

Een ander citaat: Natasha Friis Saxberg betoogt bij TEDx¹¹³ naar aanleiding van een door haar uitgebracht (Deens) boek dat in vertaling is getiteld: Homo digitalis, mapping our human basic needs with our digital behavior:

"[...] There are three universal relational structures that are the same across borders across demographics and across cultures. The first is called intimate connectedness, that's the one we have with our spouses and sweethearts. The other is relational connectedness, which we have among friends or colleagues. [...] The third and most interesting relational structure in this context is collective connectedness. That's the one we experience when we gather in groups and it can be spread online and does not need to be based on physical meeting. Collected connectedness gives us a sense of belonging during events where we feel united whether it's people protesting in the streets of Tehran, Tahrir square or [...] That gives us a sense of purpose and passion that is not matched on our daily social streams [...] makes us feel lonely [...] we can avoid becoming lonely if we believe someone will take care of us when we are in need."

De pointe van Saxberg's betoog (eveneens sociaal-wetenschappelijk van aard) lijkt te zijn dat onze gevoelens van eenzaamheid via sociale media kunnen worden verdrongen door gevoelens van 'erbij horen.' Deze stelling zou een deel van de verklaring kunnen zijn van waarom eerst SMS (1982) en later enkele andere grote sociale media zoals Wikipedia (2000), Facebook (2003), Twitter (2006) en WhatsApp (2009) zulke spectaculaire successen zouden worden. Opmerkelijk blijft het dat de grote telecomaانبieders en/of ICT-giganten die vraag kennelijk over het hoofd hebben gezien of het commerciële belang ervan hebben onderschat.

Een ander citaat komt uit de hoek van de journalistiek. Het expertisecentrum voor de journalistiek, een digitaal informatiecentrum voor de journalist wijdt een artikel¹¹⁴ aan het begrip homo digitalis:

"De vervagende grens tussen mens en machine. Nog even en je leefstijlcoach- app bepaalt dat je gaat sporten. De auto oordeelt dat je niet meer kan rijden na een vrijdagmiddagborrel. De computer grijpt in wanneer je aandacht op het werk verslapt. En zelf modificeer je straks je yoghurtbacteriën met DNA dat je via internet hebt besteld." (sic!)

Het citaat besteedt aandacht aan de kwetsbaarheid van de autonomie van wie diensten gebruikt die gedigitaliseerd zijn en waarschuwt, zo lijkt het, voor al te grote afhankelijkheid. De journalistiek beweegt zich hier in de richting van de filosofie.

113. Vindbaar achter adres <https://www.youtube.com/watch?v=xCoR0bI9mAo> (laatstelijk geraadpleegd op 18 december 2015).

114. Vindbaar achter www.expertisecentrumjournalistiek.nl/homo-digitalis/ (laatstelijk geraadpleegd op 18 december 2015).

Tegenover wat we toch maar als technologiepessimisme lezen bij de journalistiek treffen we ook onverbloemd techno-optimisme. We geven als voorbeeld een citaat van Rydell op een website die zich Mind Control noemt en gepubliceerd wordt door MindTech Sweden:¹¹⁵

"But soon the technology will not only prepare us, it will also improve. [...] A man who can move things with thought and read your mind. A man who sees more [...] There are no fantasies, the properties are within scientific reach. We have already taken the first steps towards a new man. Homo digitalis."

Hoewel wij niet zo gevoelig zijn voor dit soort beschouwingen, die er zonder veel reflectie van uit lijken te gaan dat een wereld vol machines die onze gedachten kunnen lezen een wenselijke toestand zou opleveren, vermelden we het hier volledigheidshalve, omdat de term homo digitalis voor techno-optimisten een weer heel andere betekenis gaan aannemen dan die welke wij voor ogen hebben.

Tenslotte nog een citaat dat een speculatie bevat over een tweedeling die van nog groter belang lijkt dan die welke de econoom Piketty ons heeft voorgerekend.¹¹⁶ Het citaat is ontleend aan Carsten Corneliusen, *Homo sapiens digitalis*, een boek uit 2004:¹¹⁷

"Those individuals that have evolved beyond the present social political correctness (as standard psychological beings of normative existential maturity) are about to reach a stage where they are able to decide and do what they want to become (used as a distinct psychological terminology) and they hold the power to do so [for themselves]. The rest of the world will be left in a vacuum, and if they do not evolve further and become smarter, they will stay there." (p. 29).

Onze korte verkenning naar hoe het begrip homo digitalis inmiddels op het internet is ingeburgerd leverde dus een aantal uiteenlopende resultaten, zozeer uiteenlopend dat we ons nog niet wagen aan een eigen definitie. Maar als de betekenis varieert per gebruikersgroep, heeft het begrip dan tenminste een constante functie?

2. *Waarom het begrip homo digitalis?*

Er bestaan verschillende veel beter ingeburgerde samenstellingen met de Latijnse *homo*. We laten enkele de revue passeren om na te gaan of dat

115. Te vinden achter www.mindcontrol.se/?page_id=17 (geraadpleegd op 26 december 2016).

116. Thomas Piketty, *Capital in the Twenty-First Century*, Harvard University Press 2014

117. Achter www.strategix.dk/pdf/digitalisuk.pdf (geraadpleegd op 26 december 2016) is een Engelse samenvatting te vinden.

beter licht werpt op waarom en hoe we het concept homo digitalis kunnen begrijpen en gebruiken.

Het concept *homo economicus* is in de economie een *modelmatige* eigenschap van de menselijke soort, een eigenschap waarvan de aanvaarding door de economische wetenschap niet gelijk wordt geschakeld met de psychologische werkelijkheid, maar wel noodzakelijk wordt gevonden om economische processen te kunnen beschrijven. Persky zegt het zo:

*"In economics, homo economicus, or economic human, is the concept in many economic theories of humans as rational and narrowly self-interested actors who have the ability to make judgments toward their subjectively defined ends. Using these rational assessments, homo economicus attempts to maximize utility as a consumer and economic profit as a producer. [...] The term 'economic man' was used for the first time in the late nineteenth century by critics of John Stuart Mill's work on political economy."*¹¹⁸

In het domein van de politieke economie worden de rollen omgedraaid: in samenhang met een naïeve conceptualisering van de onzichtbare hand van Adam Smith wordt de homo economicus een ideaalbeeld dat - mits nageleefd - zal leiden tot optimalisering van de welvaart. Hieronder het citaat waarnaar in het vorige citaat wordt verwezen:

*"[Political economy] does not treat the whole of man's nature as modified by the social state, nor of the whole conduct of man in society. It is concerned with him solely as a being who desires to possess wealth, and who is capable of judging the comparative efficacy of means for obtaining that end."*¹¹⁹

Met andere woorden: Occam's scheermes is toegepast op de menselijke natuur (en daarmee op de vrije wil en de menselijke waardigheid) in de economische wetenschap op een wijze die in de populair-politieke arena (en soms ook in de economische wetenschap zelf, zie hierover bijvoorbeeld Bowles (2006) of Beinhocker (2006)) de betekenis heeft verworven van *een universeel wenselijke verworvenheid* omdat de economie als geheel daar beter van zou worden. Het canonieke citaat is hier de slogan "*Greed is good*" van Gordon Gekko in de film *Wallstreet* (20th Century Fox 1987).¹²⁰

Het begrip *homo economicus* heeft – mede door de impliciete projectie van model naar norm – geleid tot heftige debatten, en doet dat nog. Wij

118. Persky (1995).

119. John Stuart Mill. "On the Definition of Political Economy, and on the Method of Investigation Proper to It," *London and Westminster Review*, October 1836. Essays on Some Unsettled Questions of Political Economy, 2nd ed. London: Longmans, Green, Reader & Dyer, 1874, essay 5, paragraphs 38 and 48].

120. Zie voor een onderbouwing van popularisering en de bijbehorende betekenisprojectie http://en.wikipedia.org/wiki/Gordon_Gekko.

mengen ons daarin niet. Maar we stellen wel vast dat het begrip *homo economicus* een centraal model is geworden voor de economische wetenschap van een rationeel handelende en denkende economische actor.

Huizinga (1938) schreef zijn *homo ludens* in het interbellum. Het is een uitzonderlijk werk voor een historicus, en heeft internationaal erkenning gevonden, onder meer door een vertaling in het Engels en een lemma in Wikipedia.

"Homo Ludens or "Man the Player" (alternatively, "Playing Man") is a book written in 1938 by Dutch historian and cultural theorist Johan Huizinga. It discusses the importance of the play element of culture and society. Huizinga suggests that play is primary to and a necessary (though not sufficient) condition of the generation of culture. Play is older than culture, for culture, however inadequately defined, always presupposes human society, and animals have not waited for man to teach them their playing. Huizinga begins by making it clear that animals played before humans. One of the most significant (human and cultural) aspects of play is that it is fun." ¹²¹

Wij menen dat de *homo ludens* een conceptualisering is die complementair is aan wat we zullen zien bij de *homo sapiens*: Huizinga bespreekt het belang van de universele predispositie van de *homo sapiens* om als *homo ludens* bij te dragen aan de beleving en ontwikkeling van zijn cultuur. Hij benadrukt daarbij vijf karakteristieken van "spelen:" als een uiting van vrijheid, van verbeelding, als buiten het normale leven staand in plaats en tijd, als ordenende activiteit, als profijtloos. Spelen in deze zin amuseert en animeert en heeft, omdat het een sociale activiteit is, onbedoeld betekenis voor een cultureel *trial en error* gebeuren. De overeenkomst van Huizinga's *homo ludens* en de *homo economicus* is dat ze beide een centrale rol vervullen bij de theorievorming over de wijzen waarop het gedrag van actoren in verschillende disciplines wordt onderzocht. De economie is gebaat bij berekenbaarheid en eenvoud. De historicus is op zoek naar rijkere analyses. Maar ook dan is het geschiedkundig perspectief op de handelende mens als een *homo ludens* een modelmatige, sterke vereenvoudiging.

Het begrip *homo sapiens* is een technische term in de biologie voor de menselijke soort, (tegenwoordig eigenlijk *homo sapiens sapiens*), en daarmee vooral een aanduiding voor individuen met dezelfde DNA structuur.

"Homo sapiens, (Latin: "wise man") the species to which all modern human beings belong. Homo sapiens is one of several species grouped into the genus Homo, but it is the only one that is not extinct [...] The name Homo sapiens was applied in 1758 by the father of modern biological classification [...], Carolus Linnaeus." ¹²²

121. Zie http://en.wikipedia.org/wiki/Homo_Ludens. (geraadpleegd op 22 februari 2015).

122. Zie <http://www.britannica.com/EBchecked/topic/1350865/Homo-sapiens> (geraadpleegd op 22 februari 2015.)

Die DNA-structuur (het genotype) bepaalt voor een belangrijk deel hoe individuen in de soort eruit gaan zien (het fenotype) en welke universele eigenschappen de individuen uit de soort zullen hebben. Deze zullen zich onder invloed van de omgeving tot individuele vermogens ontwikkelen. Vermoedelijk is het *kunnen* ontwikkelen van juridisch besef, net als het *kunnen* leren van een taal een erfelijk bepaalde, biologische predispositie.¹²³ Het individueel en feitelijk ontwikkelde juridische besef is dan dus, net als de individueel geleerde taal, deels biologisch en deels cultureel bepaald.

Het begrip *homo sapiens* gaat over het biologische deel, over de populatie, niet over een groep, en past dus in het biologische discours. Met de toename van onze kennis over evolutionaire processen, en de samenhangende popularisering ervan is het begrip ook deel gaan uitmaken van het algemene debat. Zo zijn de ongeschonden universele, biologische eigenschappen van de *homo sapiens* de noodzakelijke voorwaarden om zich tot een *homo ludens* te kunnen ontwikkelen.

Onze korte verkenning van de wijzen waarop samenstellingen met de Latijnse *homo* zich een blijvende plaats verwerven hangt, menen we, samen met het antwoord op de vraag of die samenstellingen een sleutelrol spelen in de modellering van het domein van de desbetreffende discipline. Wij gebruiken het begrip *homo digitalis* dan omdat het een centrale rol kan gaan spelen in het rechtswetenschappelijk debat.

3. *De homo digitalis als autonoom individu*

We zijn dan *de facto* op zoek naar een voor de rechtswetenschap bruikbare definitie van de *homo digitalis*. Bruikbaar in de zin dat hij geen verbazing wekt bij normaal gebruik, en dat hij een onvermijdelijk aanknopingspunt biedt voor rechtswetenschappelijke overwegingen. We menen dat die definitie daarom moet aansluiten bij wat zowel techno-pessimisten als techno-optimisten na aan het hart ligt, en wat centraal is voor het bestaande recht (dat mogelijk bedreigd wordt in de toekomst). We denken dat de individu als autonome beslisser in *digitalibus* in deze puzzel past. Daarmee wordt de *homo digitalis* een kwestie van de-mate-waarin, van de mate waarin een individu zich laat vertegenwoordigen en/of laat leiden door gedigitaliseerde processen.

Het gaat ons in deze bijdrage om verantwoorde besluitvorming, de legitimering daarvan en de rechtsbescherming in verband daarmee. In onze aanpak wordt derhalve met de term *homo digitalis* allereerst gerefereerd aan een verantwoordelijk individu, maar verder als dat zo uitkomt ook aan de individuen die deel uitmaken van instituties en instellingen, rechtspersonen, bestuursdiensten, ondernemingen en andere organisatievormen. In

123. In deze geest ook Pagel (2012).

voorkomende gevallen zal dat met zich brengen dat we dergelijke organisatievormen in het taalgebruik in minder of meerdere mate vereenzelvigen met de desbetreffende individuen die alleen of met anderen invloed hebben op de wijze waarop deze in het maatschappelijk verkeer optreden. Een andere benadering, waarbij we het begrip rigide zouden opvatten, heeft het risico dat ons blikveld te beperkt wordt en dat we geen zicht hebben op belangrijke rechtspositionele implicaties die het gevolg zijn een toeneemende verdichting van de digitale dienstverlening en van digitale organisatievormen.

We gaan dus ervan uit dat de homo digitalis als autonoom individu voor zich handelt, maar zijn ons ervan bewust dat zijn rol lijkt te verminderen en te veranderen wanneer hij optreedt als functionaris c.q. vertegenwoordiger van bijvoorbeeld een onderneming of overheidsdienst.

Appendix 2. Veiligheid, vrijheid en grondrechten

Het spreekt waarschijnlijk niet helemaal vanzelf dat ons betoog kan passen in een meer algemeen beeld van de krachten en beginselen die een rol hebben gespeeld (en nog spelen) bij de ontwikkeling van onze Westerse rechtssystemen, en de rollen (bevoegdheden, taken, plichten) die bij de ontwikkeling ervan aan het bestuur werden en worden toegekend. We menen dat het zoeken naar hoe ons betoog kan passen in wat de mainstream hierover denkt behulpzaam kan zijn om het in de rechtswetenschappelijke traditie te plaatsen.

In het onderwijs van de Leidse rechtenfaculteit wordt bij de vakgroep Encyclopedie¹²⁴ de nadruk gelegd op enkele belangrijke ontwikkelingen in het rechtsdenken over het sociaal contract. Wat ons daarbij van belang voorkomt is dat in die ontwikkeling een aantal stappen kan worden herkend die laten zien dat er een aantal centrale concepten spelen: soevereiniteit, een geweldsmonopolie, de Rule of Law, de scheiding der machten en de algemene wil van een volk.

We geven een grove, functionele schets van hoe en waarom de rol van het bestuur in de trias tot stand is gekomen, hoe die functionele positionering heeft geleid tot positiefrechtelijk bevestigde beginselen die ook steunen op moderne wetenschappelijke en economische inzichten. We hangen dit verhaal op aan enkele jaartallen

1581 Het Plakkaat van Verlatinghe: Soevereiniteit wordt voorwaardelijk
In 1581 hadden de Verenigde Provinciën er genoeg van en zwoeren Philips

124. Wat hieronder volgt is ontleend aan en geïnspireerd door een hoorcollege dat onze Leidse collega mr. dr. A.J. Kwak aan buitenlandse masterstudenten gaf in 2015, wiens commentaar op deze bijlage we in dank hebben verwerkt.

II af als hun soeverein vorst. Een deel van de tekst van het Plakkaat is veelzeggend (we citeren eclectisch uit de tekst die Wikipedia geeft) omdat er duidelijk uit wordt dat aan het einde van de zestiende eeuw iets als een rechtssysteem (op zoek naar dynamisch evenwicht tussen de belangen van de prins en van zijn onderdanen), onder voorwaardelijk gezag van een soeverein (die dus kon worden afgezet):

[...] En so wanneer hy sulx niet en doet, maer in stede van zijne ondersaten te beschermen, deselve soeckt te verdrucken, t'overlasten, heure oude vryhey, privilegien ende oude herkomen te benemen, ende heur te gebieden ende gebruycken als slaven, moet ghehouden worden niet als Prince, maer als een tyran ende voor sulx nae recht ende redene magh ten minsten van zijne ondersaten [...] voor egheen Prince meer bekent, maer verlaeten [...]

Als we aannemen dat in die tijd het bestuur onderdeel was van de bevoegdheden van de soeverein, wordt vanaf 1581 verdedigd dat wanneer de soeverein niet voor de veiligheid van zijn onderdanen zorgt, en hun verworven privileges schendt, hij rechtmatig (als tyran) kan worden afgezet. Het bestuur heeft vanaf 1581 in Nederland een functie: het beschermen van de burgers (en hun verworven rechten).

1651 Hobbes' Leviathan: Het Zwaard en het Recht – twee hiërarchieën
Soevereinen worden vervangen. Dat gebeurde ook al in 1581. Sovereinloze gemeenschappen worden onwenselijk geacht. Hobbes stelde de vraag waarom we een soeverein (of een hiërarchisch georganiseerde macht) nodig hebben. Daarzonder maatschappelijke chaos, oorlog van man tegen man

“... and the life of man, solitary, poor, nasty brutish and short ...”

Om dit alles tegen te gaan is er een soeverein nodig, die beschikt over een geweldsmonopolie (“het Zwaard”) dat de veiligheid van de burger garandeert. Veiligheid is de enige bron van legitimiteit voor Hobbes en alleen als de vrede en veiligheid niet effectief worden gehandhaafd mag de burger in verzet komen. Recht is vrijwel geheel ondergeschikt aan veiligheid, we zien dit terug in hedendaagse instituties als ‘noodtoestand’ en “noodweer.” Hobbes ziet de staat en diens soevereiniteit wel *bottom up* rustend op de redelijkheid van de burgers.

1689 Locke's Treatises on Government: van Veiligheid naar Vrijheid via de Rule of Law

Maar de organisatie in termen van soeverein met een geweldsmonopolie is niet voldoende. De soeverein kan het recht zodanig vorm geven dat de tirannie legitiem wordt. Er moet iets van doelbinding komen voor wetge-

ving. Voor Locke is het respecteren van de natuurlijke vrijheid van de burger de belangrijkste bron van legitimiteit. Locke pleit dus voor een recht op verzet tegen de staat als individuele vrijheden en eigendommen worden aangetast. Het legaliteitsbeginsel volgt als vanzelf: de burger heeft natuurlijke rechten (op veiligheid, vrijheid en eigendom). Locke zoekt het dus in een verandering van focus waar het de taak van de soeverein (en het recht) betreft: het recht is er niet om te verbieden en te beschermen, maar om een zo groot mogelijke vrijheid van burgers te garanderen. Van daaruit kunnen wettelijke regels worden geformuleerd waaraan zowel Het Zwaard als het Recht zich te houden hebben. We noemen die de Rule of Law (later worden dat de grondrechten).

1748 Montesquieu's Esprit: Scheiding der Machten, Institutionele systemen

Weer een jaar of zestig later analyseert Montesquieu welke instituties het beste bij de verschillende staatsregimes passen. Hij onderzoekt er drie, de despotie, de monarchie en de republiek. Als individuele burgerlijke vrijheid centraal staat, zo betoogt hij, ontbreekt die geheel in de despotie, is die gecentreerd rond veiligheidsmaatregelen in de monarchie en is die in de republiek afhankelijk van een goede en gescheiden organisatie van de staatsmachten: wetgeving, bestuur, rechtspraak. Opnieuw gaat het om dynamische evenwichten die elkaar in toom moeten houden, en om het maximeren van de individuele vrijheid van de burger.

1768 Rousseau's Contract: Niet het staatshoofd, maar de Rule of Law als soeverein; 1786 Democratiën beginnen te komen: We, the people ...

Rousseau maakt het verhaal rond door een kunstgreep toe te passen. Hij stelt dat groepen een enkelvoudige algemene wil hebben die gericht is op het behoud van de groep en op het algemene welzijn daarbinnen. Bij Rousseau is niet de staat, en niet het recht, maar het volk soeverein. De algemene wil moet tot wet worden gemaakt en door de staat worden gehandhaafd. Rousseau biedt zo een conceptueel kader voor de democratie. In de moderne democratiën zijn langs deze weg vrijheidsrechten (en het legaliteitsbeginsel) tot grondrecht geworden. Het concept algemene wil staat toe om aan de producten daarvan bijzondere status toe te kennen. Locke's Rule of Law kan zo in een door Rousseau geïnspireerde benadering de rol krijgen van de soeverein. In die geest wordt het bestuur dan de institutie die de opdracht heeft om de Rule of Law te verwezenlijken. We onderscheiden vaak het formele rechtsstaatsbegrip – 'rule of law' and not by men' – van het materiële rechtsstaatsbegrip waarin niet alleen het legaliteitsbeginsel maar ook een bepaalde grondrechtencatalogus tot het wezen van de rechtsstaat behoort. De in de Rule of Law gerealiseerde volkswil is zo soeverein geworden, en het bestuur daaraan dienstbaar.

2015 De homo digitalis ...

In dit verhaal over de weg naar Westerse democratieën is de verhouding burger-soeverein weergegeven als een zich ontwikkelend concept. Die ontwikkeling verliep langs steeds betere manieren om het nodig geoordeelde geweldsmonopolie te brengen naar een bestuur dat steeds minder het risico in zich bergt van geweldsusurpatie. Ten eerste door de nadruk van bestuursstaken te leggen op het beschermen van vrijheid (vanaf Locke) in plaats van veiligheid. Ten tweede door grondrechten te formuleren (de Rule of Law) die grenzen stellen aan de wetgeving (doelbinding aan verwezenlijking van vrijheid). Ten derde door het bestuur in drie onafhankelijke instituties onder te brengen, en de wetgeving en de rechtspraak los te maken van het eigenlijke bestuur (machtscheiding). Ten vierde, tenslotte, door de grondrechten als uiting te zien van de algemene wil van een volk.

In feite, en in grove lijnen, werden de Europese staten bijna allemaal tot ver in de negentiende eeuw bestuurd door nauwelijks door wetgeving ingetoomde absolute vorsten, of hun functionele equivalenten. De ideeën rond hoe regimes te verbeteren hebben in de loop der tijd vorm gekregen en zijn in de daaropvolgende periodes ook verwezenlijkt, in het bijzonder rond de Amerikaanse onafhankelijkheid, de Franse Revolutie, het Weense Congres van 1815 en de ‘democratische lente’ van 1848. In de geschetste ontwikkeling kan in grote lijnen een accentverschuiving worden waargenomen: van het primaat van de bescherming van individuele *veiligheid* naar het primaat van de bescherming van individuele *vrijheid*.

Eén en ander betekent dat de macht van het offline bestuur van de twintigste eeuw, voorafgaand aan de opkomst van de ICT,¹²⁵ werd beperkt door de wet (legaliteitsbeginsel), dat het bestuur een onafhankelijke institutie was naast de wetgever en de rechtspraak (machtscheiding) en dat het bestuur als opdracht had om de grondrechten van individuele burgers te beschermen.¹²⁶

We hebben deze beschouwing aan de ontwikkeling van onze bestuursrechtelijke arrangementen naar voren gebracht omdat we menen dat de ontwikkeling van onze samenleving van offline naar digitaal een misschien onverwachte wending neemt waar het gaat over hoe het gesteld is met de bescherming van onze individuele veiligheid en de bescherming van onze individuele vrijheid. Die twee waarden vormen een spanningsveld. Veel van onze beschouwingen over de rechtsbescherming van de homo digitalis spelen zich af tegen de achtergrond van dit spanningsveld.

125. Zie voor een analyse van de veranderende rol van de rechter in dit verband ook: Barkhuysen et al. (2014).

126. In deze geest ook Overkleeft-Verburg (1999).

Appendix 3. Iets over de *homo digitalis* (of de menselijke natuur) als voorwerp van natuurwetenschap

In dit preadvies verdiepen wij ons in de rechtspositie van de *homo digitalis*, de mens die in een gedigitaliseerde wereld zijn weg moet vinden en zich moet zien te handhaven. Het was ons inziens noodzakelijk uiteen te zetten wat we (als juristen) verder bedoelen met de notie van *homo digitalis* (in de rollen van bestuurder en bestuurd). We ontleenden daarbij inzichten aan menstyperingen zoals die in andere disciplines wel een bijzondere rol spelen, zoals de *homo economicus*, de *homo ludens*, de *homo universalis*, de *homo sapiens*, etc. We gaven al aan in welk opzicht de *homo digitalis* een bijzondere karakterisering van de mens als voorwerp van rechtswetenschappelijke studie verdient. Maar ook dat met die karakterisering het hele verhaal niet is verteld.

Natuurlijk niet, want het hele verschijnsel van maatschappelijke digitalisering was onmogelijk geweest zonder belangrijke ontwikkelingen in de natuurwetenschap. Het concept *homo digitalis* zou er zonder die ontwikkelingen helemaal niet zijn. En dat betekent dat het begrip *homo digitalis* óók een centrale (maar vermoedelijk heel andere) rol speelt voor de natuurwetenschappen. We gaan ook vanuit dit perspectief kort een aantal relevante ontwikkelingen na aan de hand van enkele (vanzelfsprekend eclectisch gekozen) jaartallen.

1687. Newton publiceert zijn *Principia* met daarin een bruikbare wiskunde voor het beschrijven van de door hem geformuleerde wetten van de mechanica en de zwaartekracht. In veel opzichten markeert dit jaartal het begin van de moderne tijd, die een natuurwetenschap inluidt die vooral mechanische verklaringen zoekt en vindt. Waar dat niet lukt wordt een intellectueel dualisme (dat Descartes al eerder filosofisch noodzakelijk vond, 1644) aantrekkelijk. Deze ontwikkeling markeert ook de kloof die tussen de natuurwetenschap en de geesteswetenschappen (waaronder we de rechtswetenschap rekenen) kon ontstaan en nog steeds de onderlinge verhoudingen domineert.

1859. Darwin publiceert zijn *On the Origin of Species*. Voor de rechtswetenschap van belang omdat er via de natuurwetenschap een argumentatielijn aan kan worden ontleend die veel van de complexiteit die we om ons heen zien verklaren kan, zonder terug te grijpen naar het beeld van een schepper. Juridisch wordt het beeld van een schepper immers traditioneel ook gebruikt om bestuurlijke soevereiniteit mee te legitimeren. Beide argumentatielijnen leiden tot zorgen over de falsificeerbaarheid. De latere ontrafeling van de structuur en werking van DNA- en RNA-moleculen hebben veel van die zorgen, voor velen, weggenomen.

1945. Von Neumann geeft het *ontwerp voor de computer* als universele rekenmachine. Aangenomen kan worden dat daarmee de digitale tijd werd ingeluid (en de homo digitalis als concept mogelijk werd) omdat dat ontwerp resulteerde in de eerste computer (en nog steeds kan worden herkend in de computers van vandaag de dag). Opmerkelijk is dat von Neumann rond die tijd ook een model van *een zelfreproducerende machine* presenteerde – waarvan later de verwantschap met onze huidige kennis over de werking van DNA en RNA is getoond.

1976. Robert May publiceert zijn “Simple mathematical models with very complicated dynamics” in *Nature*,¹²⁷ waarin hij laat zien dat heel eenvoudige mathematische modellen van situaties die voortkomen uit een eerdere versie van zichzelf tot onvoorspelbare resultaten leiden kunnen. We kiezen deze publicatie als het begin van de herkenning (en dus: bestudering) van complexiteit door de natuurwetenschappen.

Veel natuurwetenschappers beschouwen netwerken van mensen als gemeenschappen en, daarmee, als complexe, adaptieve systemen. Sommigen onthouden zich van commentaar en analyse, mogelijk omdat volledige, mathematisch oplosbare modellering van het gedrag van dergelijke systemen onmogelijk is. Anderen zien daar juist een belangrijke taak voor de wetenschap en menen dat de dynamiek in en van gemeenschappen ten minste gedeeltelijk kan worden doorgrond met behulp van de methoden en technieken complexiteitstheorieën als ontwikkeld in de exacte wetenschappen.¹²⁸

Die methoden en technieken slaan niet erg aan in de onze discipline (de rechtsgeleerdheid). Dat zou deels te wijten kunnen zijn aan de selectie van vragen en de wijzen waarop antwoorden worden gezocht. Zo is een centrale vraag bij biologen en economen hoe te verklaren dat veel mensen de neiging hebben ontwikkeld om de kosten van samenwerking voor lief te nemen, ook in die gevallen waarin de resultaten om niet beschikbaar hadden kunnen komen. Voor juristen is die vraag niet zo van belang, omdat wij altijd over kostbare samenwerking kunnen redeneren vanuit het recht (wetgeving en overeenkomsten) dat is gemaakt door en geldt voor verantwoordelijke individuen. We vinden nu eenmaal niet dat het recht een inherent, noodzakelijk voortbrengsel is van universele natuurwetten. We gaan uit van de natuurlijke predispositie in de mens tot bewuste, verantwoordelijk gedragskeuzen en vinden het idee dat die keuzen zelf gepredetermineerd zouden zijn in de oerknal nogal excentriek.

127. May (1976).

128. Bijvoorbeeld: Mitchell (2009), Lane et al. (2009), Scheffer (2009), Pagel (2012).

Het soort samenwerking dat biologen verbaast komt op een opmerkelijke wijze tot uiting bij de opbouw van de inhoud van Wikipedia en het bewaken van de kwaliteit ervan tegen ongewilde en kwaadwillig aangebrachte fouten. Belangwekkend onderzoek naar hoe die samenwerking inhoudelijk en bij de ontwikkeling en handhaving van standaarden vorm heeft gekregen, en welke rollen daarbij werden gespeeld door het formuleren en handhaven van regels werd niet gedaan door juristen, maar onder leiding van een in complexiteit geverseerde astrofysicus (die ook onderzoek deed naar rechts-culturele ontwikkelingen in het VK op basis van verschuivingen in taalgebruik in de volledige verzameling uitspraken die door de “Old Bailey” werden gedaan).¹²⁹ De ervaringen van Wikipedia en het werk van DeDeo laten zien dat, en hoe, in sommige gevallen handhaving van regels in netwerken door individuele leden uit de gemeenschap worden opgebracht.

We achten het dan ook goed mogelijk dat noties uit de niet-juridische disciplines over complexiteit voor juristen aantrekkelijk worden, wanneer duidelijk is dat de voorliggende problematiek complex is en onoplosbaar lijkende problemen oplosbaar blijken. De behandeling van bijvoorbeeld de vraagstukken van klimaatbeheersing, mensenrechten en economische uitsluiting leidt steeds vaker tot het besef dat het voorwerp van onderzoek complexe co-evoluerende netwerken vormen.¹³⁰ En dat ondersteunt het bij de bestudering ervan te hulp roepen van de modellen en de simulatietechnieken uit de wereld van de complexiteit. We denken dat die weg ook moet worden verkend bij de benadering van veel van de door ons geschetste risico's voor de homo digitalis.

We lieten al enkele voorbeelden zien van hoe complex situaties *in digitalibus* zijn. We geven hier ter illustratie drie citaten.

Het eerste citaat voert terug naar de erkenning van ons onvermogen de risico's nauwkeurig te bepalen, laat staan concrete oplossingen aan te wijzen:

Wanneer we in aanmerking nemen dat er zelfs onder de huidige, gebrekkige beveiligingsmogelijkheden een ontwikkeling gaande is van een offline wereld naar een digitale wereld menen we dat daarmee de noodzaak is ontstaan om effectief te werken aan behoud (of herstel) van vertrouwen in de betekenis van de materiële zorgvuldigheid. Die noodzaak rust op het besef dat, wanneer alle risico's die we hebben geïnventariseerd tegelijkertijd zouden gaan spelen, de gevolgen onrustbarend, om niet te zeggen: ont-

129. DeDeo (2015a), Heaberlin en DeDeo (2015), Klingenstein et al. (2014).

130. Complexiteit als van netwerken binnen gemeenschappen en als van netwerken tussen gemeenschappen – als bijvoorbeeld culturen, religies, markten, disciplines, natiestaten.

wrichtend zouden zijn. We vermoeden dat hiermee een politieke noodzaak bestaat om tot een gelaagd fundament van betrouwbare infrastructurele protocollen en diensten te geraken waarop de individuele transacties in vrijheid en veilig kunnen worden aangegaan. In elk geval, en tenminste, voor de transacties tussen burgers en overheden

Het tweede citaat is uit Morgan's schets van wat een Internet-of-Things is. Het vertaalt zich moeiteloos in de karakteristieken van een complex adaptief systeem:

"Simply put this is the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other). This includes everything from cell phones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. [...] The IoT is a giant network of connected "things" (which also includes people). The relationship will be between people-people, people-things, and things-things"

Daarnaar wordt door de natuurwetenschappen en door de rechtswetenschap op heel uiteenlopende wijzen gekeken, terwijl toch aannemelijk is dat voor de inherente problemen die het IoT gaat opleveren de rechtswetenschap en de natuurwetenschappen de handen ineen zouden moeten slaan.

Het derde citaat laat zien dat die complexiteit zich in beginsel in de termen van complex adaptieve systemen, wetenschappelijk zou kunnen laten analyseren

... dat leidt vooral tot complicaties wanneer de knooppunten in zo'n netwerk zich in een ander tempo ontwikkelen, wanneer innovatie- of handelingscycli niet synchroon lopen. Alles kent zijn tijd. Het gaat om het verwezenlijken van technologische innovatie, de behandeling van een rechtsgeschil, het aanpassen van beleid, van de wet, een cultuuromslag, etc. Dat allemaal loopt niet zonder meer synchroon. En toch hebben al de genoemde processen invloed op elkaar, als ze deel uitmaken van zo'n netwerk

Het is onze verwachting dat we samenwerking nodig hebben tussen alpha en beta voor het beter informeren van de politieke processen die uiteindelijk zullen bepalen hoe we de problemen aanpakken waarvoor de digitalisering ons stelt. In dit licht is het misschien nuttig om in herinnering te roepen dat de rechtswetenschap zich al millennia richt op het domesticeren van sociale complexiteit¹³¹

131. Te vinden achter https://en.wikipedia.org/wiki/Complex_system (geraadpleegd op 27-12-2015).

Although it is arguable that humans have been studying complex systems for thousands of years, the modern scientific study of complex systems is relatively young in comparison to conventional fields of science with simple system assumptions, such as physics and chemistry.

De natuurwetenschappelijke belangstelling voor de homo digitalis en diens maatschappelijke inbedding zou er als gevolg van het besef dat het in essentie gaat om een gedeelde belangstelling wel eens toe kunnen leiden dat de kloof wordt versmald tussen de natuurwetenschappen en de rechtswetenschap. Die kloof zelf blijft even diep, en blijft verhinderen dat we uit wat *is* kunnen afleiden wat *behoort*, maar wordt misschien door de gedeelde behoefte aan inzicht in complexiteit wel zo smal, dat we elkaar over en weer kunnen toeroepen en zelfs, soms, verstaan.

Geraadpleegde literatuur

Baase, S. (1974). IBM: Producer or predator. Reason, 4–10.

Barkhuysen, T., M. van Emmerik, B. van Ettekoven, V. Mul, R. Stijnen, en M. de Werd (2014). Adequate rechtsbescherming bij grondrechtenbeperkend overheidsingrijpen: studie naar aanleiding van de Agenda voor de Rechtspraak. Kluwer.

Beinhocker, E. D. (2006). The origin of wealth: Evolution, complexity, and the radical remaking of economics. Boston: Harvard Business School Press.

Berkhout, T. en T. van Engers (2012). Onderzoeksmethodologie voor informatiegestuurd sociaal toezicht. WFR (824).

Cliteur, P. (2002). Een sociaal grondrecht op veiligheid? niet zo'n goed idee. Regelmaat (3), 83–88.

Coase, R. H. (1937, November). The nature of the Firm. Economica 4(16), 386–405.

DeDeo, S. (2015). Conflict and computation on wikipedia: a finite-state machine analysis of editor interactions. arXiv preprint. arXiv:1512.04177.

Demsetz, H. (1969). Information and efficiency: another viewpoint. Journal of law and Economics, 1–22.

Dennett, D. en M. Kinsbourne (1992). Time and the observer: the where and when of consciousness in the brain. *Behavioral and Brain Sciences* 15, 183–247.

Dirkx, J. (2012). De zaak 'diginotar': handelde de overheid adequaat? Rapport, Rijksauditedienst.

Franken, H. (1993). Kanttekeningen bij het automatiseren van beschikkingen. Pre-advies voor de vereniging voor Administratief Recht (VAR), Alphen aan den Rijn.

Fuller, L. (1930). Legal Fictions (pts. 1-3). *Illinois Law Review* 25, 877.

Gillebaard, H. en A. Vankan (2013, September). De digitale (zelf)redzaamheid van de burger: ondersteuning bij de Digitale Overheid 2017. Dialogic.

Groothuis, M.M. (2013). Op weg naar een digitale overheid. Over waarborgen en randvoorwaarden in bestuursrechtelijk perspectief. *De Gemeentestem* 2013 (7392), 436-445.

Groothuis, M.M. (2011). De digitale overheid en de Awb. Bestuursrechtelijke aspecten van elektronische communicatie. In: Groothuis M.M., Prins J.E.J. en Schuyt C.J.M. (Red.), *De digitale overheid. Preadviezen uitgebracht voor de algemene vergadering van de VAR op 20 mei 2011*. Boom, 9-70.

Heaberlin, B. en S. DeDeo (Submitted on 6 Dec 2015). The evolution of wikipedia's norm network. <http://arxiv.org/abs/1512.01725>.

Holland, J. H. (2014). *Complexity: A very short introduction*. Oxford University Press.

Hooper, P. L., S. DeDeo, A. E. Caldwell Hooper, M. Gurven, and H. S. Kaplan (2013). Dynamical structure of a traditional amazonian social network. *Entropy* 15(11), 4932–4955.

Huizinga, J. (1938). *Homo ludens: proeve eener bepaling van het spel-element der cultuur*. Haarlem: Tjeenk Willink.

Kanne, P. en J. van den Berg (2013). Kwaliteit van de overheidsdienstverlening 2013. Technical Report G6765, TNS Nipo.

Klingenstein, S., T. Hitchcock, en S. DeDeo (2014). The civilizing process in london's Old Bailey. *Proceedings of the National Academy of Sciences* 111(26), 9419–9424.

Lane, D., D. Pumain, S. E. van der Leeuw, and G. West (2009). Complexity perspectives in innovation and social change. Number 7 in *Methodos*. Springer Science & Business Media.

Loos, E. (2010, 25 juni). De oudere: Een digitale immigrant in eigen land? Een verkenning naar toegankelijke informatievoorziening (oratie UvA).

Martijn, M. (2014). Politie en inlichtingendiensten kunnen via een achterdeur bij gegevens van de belastingdienst. *De Correspondent* 30 september.

Martijn, M. (2015). Baas belastingdienst over big data: Mijn missie is gedragsverandering. *De Correspondent* (21 april).

Martijn, M. en M. Goslinga (2015). Hoe fraude het nieuwe terrorisme werd. *De Correspondent* 30 april.

May, R. M. (1976). Simple mathematical models with very complicated dynamics. *Nature* 261(5560), 459–467.

Mayer-Schönberger, V. en K. Cukier (2013). *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.

Mitchell, M. (2009). *Complexity: a guided tour*. Oxford University Press, USA.

Mommers, L., G.-J. Zwenne, en B. Schermer (2010a). Het best bewaarde geheim van de raadkamer, *NJB* 2010, 1692, a . 32. *NJB* 1692(32).

Mommers, L., G.-J. Zwenne, en B. Schermer (2010b). Naschrift. *NJB* 1696(36).

Morgan, J. (2014). A simple explanation of the internet of things. *Forbes* (13 May).

Onderzoeksraad voor Veiligheid (2012). *Het DigiNotarincident: waarom digitale veiligheid de bestuurstafel te weinig bereikt*. Onderzoeksraad voor Veiligheid.

Overkleeft-Verburg, G. (1999). De algemene wet bestuursrecht en de (beperking van) de grondrechten. In H. Kummeling (Ed.), *Het bestuursrecht als agenda voor het staatsrecht*, pp. 129–153. Kluwer.

Overkleeft-Verburg, G. (2014, augustus). De belastingdienst en zijn digitale burger: spanning tussen ambities, uitvoeringsrealiteit en het juridisch kader. *Maandblad Belasting Beschouwingen* (7-8).

Page, W. H. en J. E. Lopatka (2009). *The Microsoft case: antitrust, high technology, and consumer welfare*. University of Chicago Press.

Pagel, M. (2012). *Wired for culture: origins of the human social mind*. WW Norton & Company.

Panteia (2015) *Burgers tussen wal en schip: Het voorkomen en oplossen van knelpunten bij de (digitale) overhead*, Panteia, Zoetermeer.

Persky, J. (1995). Retrospectives: the ethology of homo economicus. *The journal of economic perspectives*, 221–231.

Philippart, R. (2010). Toegankelijkheid van rechtspraak. *NJB* 1696(36).

Scheffer, M. (2009). *Critical transitions in nature and society*. Princeton Univ Pr.

Schmidt, A.H.J. (2009). Radbruch in cyberspace: About law-system quality and ICT innovation. *Masaryk UJL & Tech.* 3, 195.

Schmidt, A.H.J. (2010). Met de kennis van nu, en met de rechtswetenschap als bril: enkele gedachten over de cyberpest (afscheidsrede).

Van der Hoek, F. (2010). Huidige opzet van rechtspraak.nl zo slecht nog niet. *NJB* 1696(36).

Van Opijnen, M. (2014). *Op en in het web. Hoe de toegankelijkheid van rechterlijke uitspraken kan worden verbeterd*, (diss. UvA). Boom Juridische uitgevers.

Wieringa, T. (2005). Niemands meester, niemands knecht. De Gids (<http://www.de-gids.nl/artikel/niemands-meester-niemands-knecht>) Kousbroek-lezing.

Williamson, O. E. (2005). The economics of governance. *American Economic Review* 95(2), 1–18.

WRR (2011). *iOverheid*. Rapport 86, WRR, Den Haag / Amsterdam.

Zhang, K. en A. H. J. Schmidt (2015). Thinking of data protection law's subject matter as a complex adaptive system: A heuristic display. *Computer Law & Security Review* 31(2), 201–220.

Zwenne, G.-J. en W. Steenbruggen (2015). Privacyvoorwaarden voor de *iOverheid*: Vuistregels voor wet- en regelgevers met betrekking tot overheidsinformatiesystemen. *Regelmaat* (1), 17–36.

Zwenne, G.-J. (2009). Over kopieerbeperkingen in elektronisch bekendgemaakte besluiten. *Tijdschrift voor internetrecht* (2).

Zwenne, G.-J. (1998). Belastingheffing en informatieverplichtingen: reikwijdte en begrenzing van informatiebevoegdheden in de verhouding tussen belastingdienst en banken. Diss. Leiden.

Zwenne, G.-J. (2011). Redactioneel. *Tijdschrift voor internetrecht* 1.

Zwenne, G.-J. (2013a). De verwaterde privacywet (inaugurele rede).

Zwenne, G.-J. (2013b). Nogmaals enige opmerkingen over overheids-internet-publicatie-beleid. *Tijdschrift voor internetrecht* 3.

Zwenne, G.-J. en A.H.J. Schmidt (2008). Opmerkingen bij het wetsvoorstel wet bewaarplicht telecommunicatiegegevens. *Mediaforum-Amsterdam* 20(7), 278.

