

# Opwaarderen

Borgen van publieke waarden  
in de digitale samenleving





**Bestuur van het Rathenau Instituut**

mw. G.A. Verbeet (voorzitter)

prof. dr. E.H.L. Aarts

prof. dr. ir. W.E. Bijker

prof. dr. R. Cools

dr. J.H.M. Dröge

dhr. E.J.F.B. van Huis

prof. dr. R.M. Letschert

prof. dr. ir. P.P.C.C. Verbeek

prof. dr. M.C. van der Wende

dr. ir. M.M.C.G. Peters (secretaris)



Opwaarderen  
Borgen van publieke waarden in de digitale samenleving

Linda Kool, Jelte Timmer, Lambert Royakkers en Rinie van Est

Rathenau Instituut  
Anna van Saksenlaan 51  
Postadres: Postbus 95366  
2509 CJ Den Haag  
Telefoon: 070-342 15 42  
E-mail: [info@rathenau.nl](mailto:info@rathenau.nl)  
Website: [www.rathenau.nl](http://www.rathenau.nl)  
Uitgever: Rathenau Instituut

Redactie: Science stories  
Illustraties: Ridders Infographics  
Foto cover: iStock  
Opmaak: Rathenau Instituut  
Druk: Rathenau Instituut

Bij voorkeur citeren als:

Kool, L., J. Timmer, L. Royakkers en R. van Est, *Opwaarderen - Borgen van publieke waarden in de digitale samenleving*. Den Haag, Rathenau Instituut 2017

Het Rathenau Instituut heeft een Open Access beleid. Rapporten, achtergrondstudies, wetenschappelijke artikelen, software worden vrij beschikbaar gepubliceerd. Onderzoeksgegevens komen beschikbaar met inachtneming van wettelijke bepalingen en ethische normen voor onderzoek over rechten van derden, privacy, en auteursrecht.

© Rathenau Instituut 2017

Verveelvoudigen en/of openbaarmaking van (delen van) dit werk voor creatieve, persoonlijke of educatieve doeleinden is toegestaan, mits kopieën niet gemaakt of gebruikt worden voor commerciële doeleinden en onder voorwaarde dat de kopieën de volledige bovenstaande referentie bevatten. In alle andere gevallen mag niets uit deze uitgave worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie of op welke wijze dan ook, zonder voorafgaande schriftelijke toestemming.

# Voorwoord

Op mijn dagboek zat een slotje. Ik kon schrijven wat ik wilde want niemand die het zag. Digitalisering maakt hier een einde aan. Je e-reader leest over je schouder mee en weet welke passages je interessant vindt. En het speelgoed van je kind is tegenwoordig zo *smart* dat de fabrikant via internet meeluistert. Is dat erg? Ja.

De voor u liggende studie 'Opwaarderen - Borgen van publieke waarden in de digitale samenleving' toont hoe de verregaande digitalisering van de samenleving fundamentele ethische en maatschappelijke vragen oproept. Het laat zien dat de overheid, de toezichthouders, het bedrijfsleven en de samenleving nog niet voldoende zijn toegerust om met deze nieuwe vragen om te gaan. Daardoor komen belangrijke publieke waarden en mensenrechten als privacy, gelijke behandeling, autonomie en menselijke waardigheid onder druk te staan.

Het Rathenau Instituut deed dit onderzoek naar aanleiding van de 'motie Gerkens' (Eerste Kamer, 23 september 2014). De senaat vermoedde dat belangrijke waarden in het geding zijn bij digitalisering. Ons onderzoek bevestigt dit.

Het Rathenau Instituut is dertig jaar geleden opgericht om onderzoek te doen naar nieuwe wetenschap en technologie en hoe die de samenleving beïnvloeden. Destijds was automatisering een belangrijk issue. Nu spreken we van digitalisering. Vorig jaar analyseerden we de invloed van deze ontwikkeling op de arbeidsmarkt en publiceerden we onder andere over big data, data in het medische domein en digitale coaches.

Nu onderzochten we breed welke technologieën de komende jaren naar verwachting de digitale samenleving verder vormgeven, welke maatschappelijke en ethische uitdagingen die ontwikkelingen oproepen en in hoeverre de omgang van die uitdagingen al maatschappelijk en politiek geagendeerd is en ook institutioneel verankerd. We identificeren blinde vlekken, schrijven welke acties nodig zijn en gaan in op de eventuele rol van een commissie.

Ik wil hierbij de Eerste Kamer bedanken voor hun kennisvraag. Daarnaast dank ik de medewerkers van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en de begeleidingscommissie: Corien Prins, Jeroen van den Hoven, Inez de Beaufort, Victor Bekkers, Heleen Janssen en Meine Henk Klijnsma. We hopen dat onze studie verhelderend en activerend werkt in de toekomstige discussies.

De dagboeken van nu zijn digitaal. Het slotje is weg. Maar we staan niet machteloos. Met de juiste acties vanuit overheid, bedrijfsleven en maatschappelijk middenveld kunnen we op een verantwoorde manier de digitalisering verder vormgeven.

Melanie Peters  
Directeur Rathenau Instituut

# Samenvatting

**De verregaande digitalisering van de samenleving roept fundamentele ethische en maatschappelijke vraagstukken op. Overheid, bedrijfsleven en samenleving zijn nog niet adequaat uitgerust om met deze nieuwe vragen om te gaan. Daardoor komen belangrijke publieke waarden en mensenrechten als privacy, gelijke behandeling, autonomie en menselijke waardigheid onder druk te staan. Grote inspanningen in alle geledingen van de overheid en maatschappij zijn nodig om de digitalisering van de samenleving in goede banen te leiden. Maar we staan niet machteloos, met de juiste acties vanuit overheid, bedrijfsleven en maatschappij, kunnen we de digitale samenleving een verantwoorde opwaardering geven.**

## **Motie Gerkens: onderzoek wenselijkheid commissie**

Internetbots manipuleren het politieke debat voor de presidentiële verkiezingen in de Verenigde Staten, bankmedewerkers verliezen in groten getale hun baan nu computers hun taken overnemen en softwareprogramma's helpen rechters de kans te berekenen dat een verdachte weer de fout in gaat, maar blijken ongemerkt te discrimineren. Digitale technologie reikt tot in de haarvaten van de samenleving en roept overal fundamentele maatschappelijke en ethische vragen op. Hoe kunnen we met deze vragen omgaan en de mogelijkheden die digitalisering de maatschappij biedt optimaal benutten? Het Rathenau Instituut deed op verzoek van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en de Eerste Kamer onderzoek naar deze vraag. Dit naar aanleiding van een motie ingediend in de Eerste Kamer van het lid Gerkens (motie Gerkens 23 september 2014). De motie verzoekt de regering het Rathenau Instituut te vragen *'de wenselijkheid van een commissie die kan adviseren over de ethische kant van de digitalisering van de samenleving'* te onderzoeken. De motie verwijst daarbij naar de opkomst van het Internet of Things dat zowel voor kansen als bedreigingen zorgt. Uit de motie blijkt dat bij de Kamer het gevoel leeft dat bij digitalisering belangrijke waarden in het geding zijn, aangezien zij niet alleen spreekt van technologische effecten van digitalisering, maar ook van *'maatschappelijke, sociaal juridische en sociaal psychologische'* effecten. Voorliggend onderzoek van het Rathenau Instituut ondersteunt die observatie van de Kamer.

## **Onderzoeksvragen**

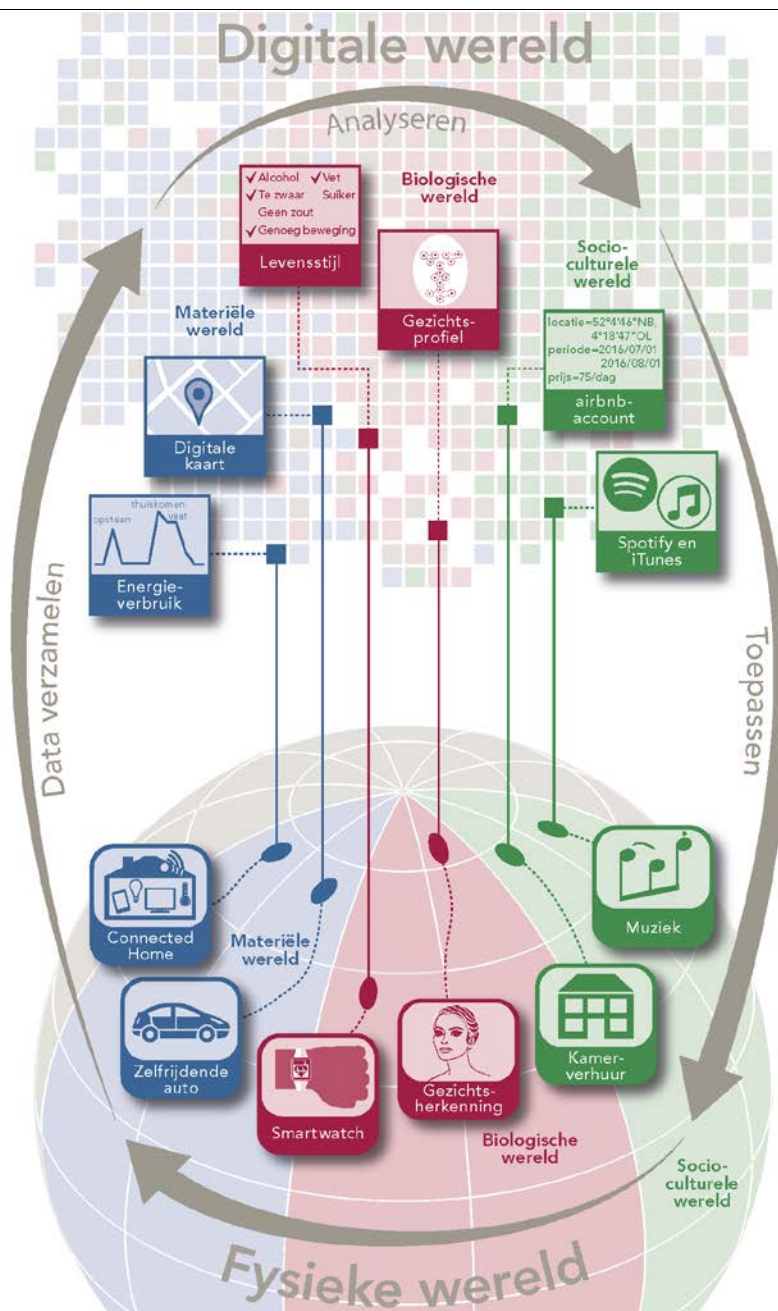
Het Rathenau Instituut onderzocht welke technologieën de komende jaren naar verwachting de digitale samenleving verder vormgeven, welke maatschappelijke en ethische uitdagingen die ontwikkelingen oproepen en in hoeverre de omgang van die uitdagingen ook institutioneel verankerd is (oftewel, de governance van ethische en maatschappelijke uitdagingen rond digitalisering). Het gaat daarbij om vragen als: welke kwesties pakken bestaande Nederlandse instituties wel of niet op, en op welke manier? Zijn er blinde vlekken ten aanzien van de omgang met (nieuwe) ethische en maatschappelijke kwesties? Welke rol kan een commissie daarin spelen?



### De nieuwe digitaliseringsgolf

De begrippen digitalisering en Internet of Things refereren aan een groot cluster van digitale technologieën, zoals robotica, kunstmatige intelligentie en algoritmen en big data, digitale platformen, biometrie, persuasieve technologie, augmented reality en virtual reality. Samen zorgen zij voor een nieuwe golf van digitalisering. Steeds meer onderdelen uit de fysieke wereld krijgen een virtuele representatie. Daardoor ontstaat op steeds meer plekken een continue terugkoppeling tussen de fysieke en de virtuele wereld, waarmee producten of diensten direct worden aangepast op basis van analyse van digitale gegevens (zie figuur 1).

**Figuur 1** Nieuwe fase in de digitale samenleving



### **Publieke waarden in het geding**

De nieuwe golf van digitalisering leidt aldus tot een wereld waarin continu terugkoppelen en real-time (bij)sturen een steeds belangrijker uitgangspunt is van diensten. Belangrijke publieke waarden als gelijke behandeling, privacy, autonomie en menselijke waardigheid komen daardoor onder druk te staan, blijkt uit onze analyse. Ook recente nieuwsberichten maken dit duidelijk. Zo blijken softwareprogramma's die rechters in de Verenigde Staten bijstaan door de kans te berekenen dat een verdachte opnieuw de fout ingaat, in sommige gevallen te discrimineren. De inzet van software om te bepalen waar extra politie-inzet nodig is, kan leiden tot een selffulfilling prophecy: daar waar meer politie is, ziet men meer vergrijpen. Die gegevens neemt de computer weer mee in haar analyse, waardoor het programma verwacht dat er op die locatie meer criminaliteit zal zijn. Datasurveillance kan leiden tot onbewuste beïnvloeding van de eigen identiteit en zogenaamde 'filter bubbels' waarin gebruikers alleen suggesties voor nieuws, informatie en contacten krijgen die passen bij hun voorgaande gedrag, keuzes en interesses. Tot slot stelt de inzet van robots en software in de zorg, rechtspraak, bankwezen en andere sectoren de urgente vraag wat we aan robots willen overlaten en wat de minimale menselijke betrokkenheid moet zijn om te kunnen spreken van bijvoorbeeld betekenisvolle, menswaardige zorg of betekenisvol verantwoordelijkheid afleggen. Daar komt bij dat publieke diensten in toenemende mate afhankelijk zijn van software die door private partijen ontwikkeld wordt, waardoor het lastig te achterhalen is welke keuzes de software maakt, en welk effect dat heeft. Zal de rechter of dokter in de ene provincie die gebruik maakt van systeem X tot andere uitspraken komen dan een andere rechter of dokter die gebruik maakt van systeem Y?

### **Blinde vlekken in het governancelandschap**

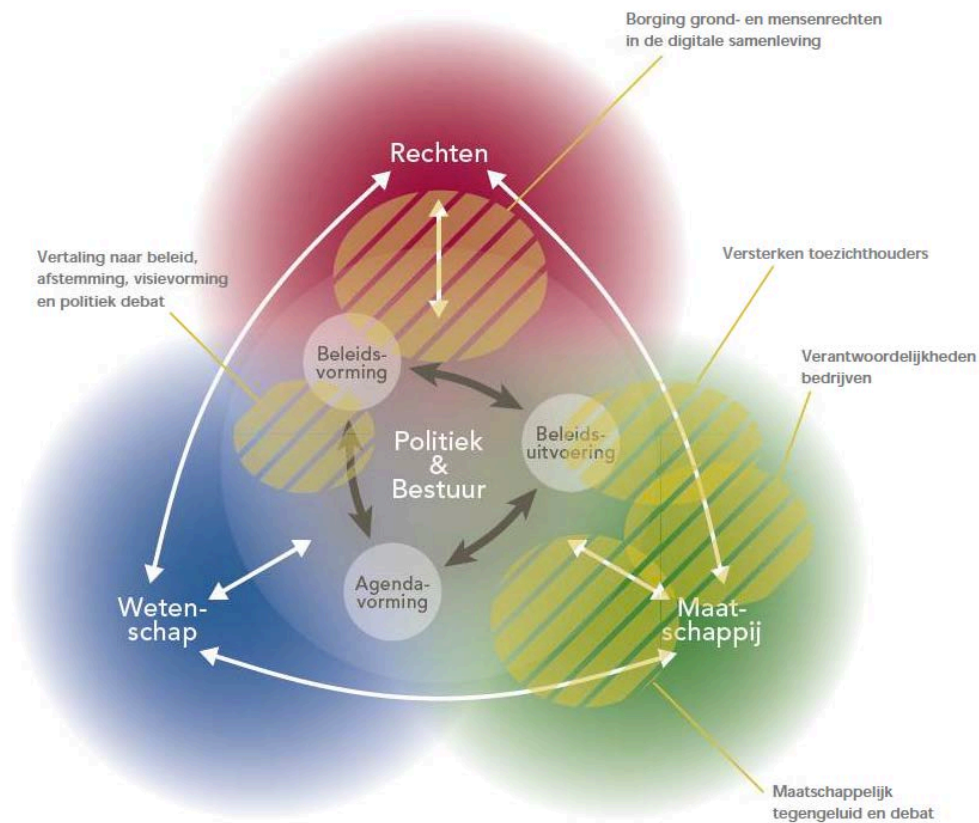
De nieuwe digitaliseringsgolf brengt dus nieuwe ethische en maatschappelijke uitdagingen met zich mee. Hierbij zijn belangrijke publieke waarden in het geding die nauw verwant zijn aan grond- en mensenrechten. Dat roept de vraag op of onze huidige wettelijke kaders en toezichtsarrangementen voldoende zijn toegerust om deze fundamentele rechten adequaat te beschermen. Het Rathenau Instituut onderzocht in deze studie de ethische en maatschappelijke uitdaging van digitalisering en in hoeverre de omgang met nieuwe maatschappelijke en ethische kwesties institutioneel verankerd is. Het bracht in een uitgebreide analyse in kaart, welke actoren voor welke kwesties aandacht vragen en welke acties zij nemen om deze uitdagingen het hoofd te bieden. Daarbij is gekeken naar de rol van de wetenschap (welke kwesties signaleren zij), de rol van grond- en mensenrechten, de rol van het maatschappelijk middenveld en de rol van politiek en bestuur bij agendavorming, beleidsbepaling en –uitvoering.

Onze analyse van het governancelandschap laat zien dat de bescherming van publieke waarden op dit moment sterk tekort schiet. Digitalisering leidt tot conceptuele verwarring over welke regels gelden en over hoe deze moeten worden toegepast. In sommige gevallen zien we dat bestaande kaders daardoor (aanvankelijk) niet worden toegepast terwijl deze wel van toepassing zijn. In andere gevallen zien we dat digitalisering vraagt om nieuwe kaders over hoe belangrijke waarden worden geborgd in de digitale samenleving. Op verschillende onderdelen van het landschap zien we dat er blinde vlekken zijn ontstaan (zie figuur 2):

- Vertaling van nieuwe maatschappelijke en ethische vraagstukken naar beleid, interdepartementale afstemming en coördinatie op digitalisering, en het politieke debat over die nieuwe vraagstukken.

- Borging van grond- en mensenrechten in de digitale samenleving.
- Versterken van toezichthouders en zorgen voor onderlinge afstemming tussen toezichthouders.
- Nieuwe verantwoordelijkheden van ontwikkelaars van digitale diensten en producten.
- Organiseren van maatschappelijk tegengeluid: versterken maatschappelijk middenveld, kennis en vaardigheden van burgers en maatschappelijk debat over digitalisering.

**Figuur 2** Blinde vlekken in het governancelandschap



Rathenau Instituut

Het gaat op al deze punten met name over de nieuwe prangende maatschappelijke en ethische vraagstukken die de inzet van kunstmatige intelligentie, robotica en het Internet of Things oproepen, bijvoorbeeld over gelijke behandeling, menselijke waardigheid, verantwoordelijkheid en ongelijke machtsverhoudingen tussen consumenten en bedrijven of tussen burgers en overheden. Denk aan digitale dienstverleners (bijvoorbeeld in de deeleconomie of sociale media) met een dominante marktpositie, waarvoor gebruikers nauwelijks alternatieven hebben en waarvan zij steeds afhankelijker zijn voor inkomsten of informatie. Op deze gebieden zijn governancestructuren nog niet uitgekristalliseerd blijkt uit ons onderzoek: het maatschappelijk debat moet zich hier nog meer vormen, en in het politiek-bestuurlijke domein worden gesignaleerde kwesties niet omgezet in concrete beleidsacties. Op het gebied van privacy en de bescherming van persoonsgegevens is dit governancestelsel meer gevormd. Hoewel ook hier fundamentele vragen blijven spelen, hebben burgers, overheid en bedrijfsleven steeds meer aandacht voor privacybescherming. De verantwoordelijke toezichthouder krijgt meer mogelijkheden en ook op Europees niveau is de

regelgeving aangescherpt. Verschillende overheidsprogramma's en programma's van het maatschappelijk middenveld zetten in op het stimuleren van digitale vaardigheden en veilig digitaal gedrag. Maar voor de impact van digitalisering op publieke waarden als gelijke behandeling, menselijke waardigheid en autonomie is slechts beperkt aandacht.

### **Opwaarderen: Actieprogramma voor een verantwoorde digitale samenleving**

Digitale innovaties ontwikkelen zich razendsnel. Digitalisering dringt door tot in de haarvaten van de samenleving. De voortdurende technische upgrades creëren tal van nieuwe mogelijkheden voor economie en samenleving. Maar het leidt ook tot fundamentele maatschappelijke en ethische vragen. Essentiële publieke waarden komen door de digitalisering van de samenleving onder druk te staan. Alle sectoren van de samenleving krijgen te maken met digitaliseringsvraagstukken en bijbehorende ethische en maatschappelijke uitdagingen. Het is tijd om de fundamentele impact van digitalisering op de samenleving te onderkennen en ervoor te zorgen dat publieke waarden en grondrechten in het digitale tijdperk worden geborgd. Dat vraagt om een upgrade, of opwaardering, van het governancestelsel. Deze opwaardering verwijst naar de benodigde versterking van het governancestelsel, door het structureel borgen van maatschappelijke en ethische waarden.

Deze opwaardering vereist dat alle partijen in de maatschappij in actie komen om digitalisering in goede banen te leiden. Het is onverantwoordelijk om als overheid, bedrijfsleven en als maatschappij van de fundamentele impact van digitalisering weg te kijken. Bij al deze actoren liggen zodoende verantwoordelijkheden om met de maatschappelijke en ethische aspecten van digitalisering om te gaan. Het startschot dient te worden gegeven door de overheid, maar het bedrijfsleven en het maatschappelijk middenveld behoren tegelijkertijd stappen te ondernemen.

Onze centrale conclusie is dan ook dat de Eerste Kamer **terecht haar zorgen uit over de ethische en maatschappelijke impact van digitalisering** in de motie Gerkens. De Eerste Kamer vraagt zich daarbij af in hoeverre het wenselijk is om een commissie in te stellen die kan adviseren over de ethische kanten van de digitale samenleving. Onze analyse laat zien dat **om essentiële publieke waarden te borgen, het governancestelsel op het terrein van de maatschappelijke en ethische aspecten van digitalisering op meerdere plekken substantieel dient te worden versterkt.**

Een commissie alleen kan de blinde vlekken in het governancestelsel niet oplossen. Een complex probleem als de versterking van het governancestelsel vereist dat alle partijen hun verantwoordelijkheid nemen en zich gezamenlijk inzetten voor de borging van publieke waarden in de digitale samenleving. Met het instellen van een commissie bestaat tevens het risico dat problemen in de praktijk bij de commissie worden 'geparkeerd' en partijen in het veld en op politiek-bestuurlijk niveau een (te) afwachtende houding aannemen. Bovendien heeft voorliggende studie het voorwerk van een dergelijke commissie reeds uitgevoerd. De studie brengt in kaart welke maatschappelijke en ethische digitaliseringsvraagstukken op ons afkomen, en waar in het governancestelsel blinde vlekken liggen om die vraagstukken het hoofd te bieden. Het biedt tevens handelingsperspectieven voor alle betrokken partijen om het governancestelsel te versterken.

**De belangrijkste boodschap van het Rathenau Instituut is dan ook dat de overheid, het bedrijfsleven en het maatschappelijk middenveld nu actie dienen te ondernemen om het governancelandschap te versterken en zo publieke waarden in de digitale samenleving te kunnen blijven borgen.**

We stellen een vijftal acties voor waarmee beleidsmakers, bedrijven en maatschappelijke organisaties het governancelandschap verantwoord kunnen opwaarderen:

1. Stel een interdepartementale werkgroep in die toewerkt naar een kabinetsvisie op de omgang met de maatschappelijke en ethische betekenis van digitalisering, en zorgt voor politiek-bestuurlijke coördinatie.
2. Versterk de rol en positie van toezichthouders.
3. Stel een "Digitaliseringsakkoord" op om commitment en verantwoordelijkheden van bedrijven, overheid, en maatschappelijke actoren omtrent de borging van publieke waarden in de digitale samenleving vast te leggen.
4. Organiseer een nationale dialoog over de betekenis van digitalisering voor de borging van publieke waarden
5. Zorg voor periodieke politieke discussie in Eerste en Tweede Kamer over de governance van maatschappelijke en ethische digitaliseringsvraagstukken.

Elke actie valt uiteen in een aantal specifieke actiepunten die we hieronder toelichten.

### **1. Stel een interdepartementale werkgroep in die toewerkt naar een kabinetsvisie op de omgang met de maatschappelijke en ethische betekenis van digitalisering**

Actiepunten voor de interdepartementale werkgroep:

- Zorg voor coördinatie van en overkoepelende visievorming op de maatschappelijke en ethische impact van digitalisering en de borging van publieke belangen.
- Verken hoe grondrechten in het digitale tijdperk kunnen worden geborgd. Hierbij is het van belang om verbinding te zoeken met en oog te houden voor initiatieven op Europees niveau, bijvoorbeeld bij de Raad van Europa.

### **Coördinatie en visievorming**

De vertaling van de gesignaleerde ethische en maatschappelijke vraagstukken naar een coherent en domeinoverstijgend beleid verloopt moeizaam. Een interdepartementale werkgroep is nodig om toe te werken naar een kabinetsvisie op de governance van maatschappelijke en ethische digitaliseringsvraagstukken, en deze op integrale en strategische wijze binnen de overheid te beleggen. De werkgroep kan zorgen voor coherentie van de vraagstukken die beleidsoverstijgend zijn. De werkgroep kan er ook voor zorgen dat het besef van de betekenis van digitalisering voor de borging van publieke waarden groeit binnen de overheid, en dat verschillende ministeriële departementen gestimuleerd worden om de betekenis van nieuwe maatschappelijke en ethische vragen op hun terrein te doordenken en te adresseren.

### **Borging van grondrechten**

Het politiek-bestuurlijke domein heeft de verantwoordelijkheid om de betekenis van digitalisering voor de borging van grondrechten te monitoren. Discussies in Nederland concentreerden zich op de

vraag of en hoe, het recht op privacy, vertrouwelijke communicatie en de vrijheid van meningsuiting aangepast zouden moeten worden in het licht van digitalisering. Recent zijn er initiatieven op Europees niveau genomen (bijvoorbeeld door de Raad van Europa, maar ook door het Europees Parlement). Die onderzoeken wat de opkomst van technologieën als AI, robotica, en het Internet of Things betekenen voor de bescherming van fundamentele rechten. Voor biotechnologie en gentechnologie is bijvoorbeeld in 1997 op initiatief van de Raad van Europa een apart verdrag opgesteld (Verdrag van Oviedo). Ondanks het brede toepassingsbereik van het Europees Verdrag voor de Rechten van de Mens (EVRM), achtte de Raad van Europa het destijds noodzakelijk om zich expliciet te richten op ontwikkelingen in de bio- en gentechnologie. Nu speelt de vraag of er een vergelijkbaar verdrag nodig is voor de bescherming van grondrechten met betrekking tot de nieuwe golf van digitalisering (Van Est & Gerritsen nog te verschijnen). Ook Nederland dient de betekenis van digitalisering voor grondrechten te verkennen, en kennis te nemen van (en verbinding te zoeken met) de Europese initiatieven die lopen op dit gebied. Ook hier ligt een taak voor de interdepartementale werkgroep.

## 2. Versterk rol en positie toezichhouders

Actiepunten:

- Toezichhouders: neem kennis van nieuwe maatschappelijke en ethische vraagstukken.
- Toezichhouders: verken hoe vanuit het huidige mandaat invulling gegeven kan worden aan deze nieuwe vraagstukken: welke regels zijn van toepassing, welke instrumenten hebben toezichhouders tot hun beschikking, welke capaciteit/kennis is nodig?
- Toezichhouders: stem in gezamenlijk overleg af wie waar verantwoordelijk voor is, en treed waar nodig gezamenlijk op.
- Overheid: bouw voorwaarden in, en vervul de rol van launching customer.

Alle toezichhouders krijgen te maken met nieuwe digitaliseringsvraagstukken, of het nu gaat om kwesties als privacy, discriminatie, machtsverhoudingen, of om menselijke waardigheid. Alle toezichhouders dienen zich te oriënteren op de vraag, hoe zij op hun terrein praktisch vanuit hun huidige mandaat invulling kunnen geven aan nieuwe ethische en maatschappelijke digitaliseringsvraagstukken. Daarbij is onderlinge afstemming van groot belang. Doordat digitalisering verschillende sectoren doorkruist, zal het handavingsdomein van verschillende toezichhouders regelmatig overlappen. Toezichhouders dienen daarom overleg te voeren over de manier waarop zij worden geconfronteerd met digitalisering, hoe het toezicht wordt georganiseerd en waar verantwoordelijkheden van verschillende toezichhouders liggen.

Oriëntatie op digitale vraagstukken wil niet per se zeggen dat er een nieuwe toezichhouder of nieuwe wet- en regelgeving nodig is. Vaak biedt bestaande wet- en regelgeving al een kader, zoals de Algemene Verordening Gegevensbescherming een kader biedt om automatische beslissingen door algoritmen onder de loep te nemen. Soms zullen het huidige mandaat en de instrumenten van een toezichthouder voldoende zijn, soms zal aanpassing nodig zijn.

Bij het versterken van de positie van de toezichhouders dient men bovendien voor ogen te houden dat het niet alleen draait om het kennismaken van nieuwe vraagstukken, en capaciteit opbouwen om deze vraagstukken op te pakken, maar ook om de vraag of de randvoorwaarden voldoende

aanwezig zijn om dat te kunnen doen. De overheid kan normerende kaders opstellen waaraan de aanschaf, ontwerp en inrichting van systemen moeten voldoen, en waar toezichthouders en handhavers op kunnen toetsen. Bijvoorbeeld door vast te stellen, hoe een software-ontwikkelaar verantwoording kan afleggen over de werkwijze van complexe algoritmen, zodat software-ontwikkelaars dat in het ontwerp van het systeem inbouwen. Op deze manier wordt duidelijk welke systemen in welke situaties aan bepaalde transparantievoorwaarden moeten voldoen. Dat speelt nog sterker wanneer het gaat om (semi)publieke diensten en digitale systemen in de zorg, het onderwijs, het rechtssysteem en dergelijke. De overheid dient daar op te treden als hoeder van publieke belangen. Door toenemende servitization (zie hoofdstuk 3) zijn systemen van publieke diensten steeds vaker in handen van private partijen, waardoor overheid, toezichthouders en handhavers vaak onvoldoende zicht hebben op en onvoldoende mogelijkheden hebben om controle uit te oefenen op de werking en effecten van deze systemen. Het moet mogelijk zijn om de inrichting van het systeem en de uitwerking daarvan te controleren. De overheid dient zich hiervan bewust te zijn bij de aanbesteding van digitale systemen, en hiertoe van tevoren voorwaarden voor op te stellen.

### **3. Stel een “Digitaliseringsakkoord” op om commitment en verantwoordelijkheden van bedrijven, overheid, en maatschappelijke actoren omtrent de borging van publieke waarden in de digitale samenleving vast te leggen.**

Actiepunten voor het Digitaliseringsakkoord:

- Bedrijven: zet de zorgplicht centraal om rekening te houden met maatschappelijke en ethische vraagstukken van digitale producten en diensten.
- Bedrijven en brancheorganisaties: zorg voor een praktische invulling van de zorgplicht via gedragscodes.
- Bedrijven, brancheorganisaties en wetenschap: verken en leer van bestaande tools en structuren die het bedrijfsleven kunnen helpen om met ethische impacts om te gaan. Privacy impact assessments kunnen als voorbeeld dienen voor een ethical impact assessment.
- Overheid en wetenschap: investeer via onderzoeksfinanciering en innovatiebeleid in verkenning en aanpak maatschappelijke en ethische implicaties van nieuwe technologie.
- Overheid: onderzoek hoe tegengelijk van niet-gouvernementele organisaties en burgers kan worden versterkt (bijvoorbeeld met class actions, of door te onderzoeken in hoeverre het wenselijk is het verbod grondwettelijke toetsing op te heffen).
- Overheid, bedrijven en maatschappelijk middenveld: meer inzetten op digitale vaardigheden in het onderwijs (jongeren en professionals).
- Overheid, bedrijven en maatschappelijk middenveld: verbreed mediawijsheid (inzicht in werking nieuwe technologie).

In samenwerking met de overheid zullen het bedrijfsleven, het maatschappelijk middenveld en burgers tevens stappen moeten ondernemen om publieke waarden in de digitale samenleving, nu en in de toekomst, te kunnen borgen. Dat kan via een “Digitaliseringsakkoord” waarin partijen vastleggen hoe zij de digitale samenleving samen een ‘humaan gezicht’ kunnen geven. Voor het opstellen van een Digitaliseringsakkoord is het van belang dat er draagvlak is bij bedrijven en deelnemende stakeholders. Voor het proces kan gekeken worden naar de aanpak die is gevolgd bij de totstandkoming van eerdere akkoorden, zoals het Energieakkoord.

### *Belang van een Digitaliseringsakkoord*

Het realiseren én uitvoeren van een dergelijk akkoord is van cruciaal belang voor Nederland. Maatschappelijke en ethische kwesties worden, net als bij biotechnologie, belangrijke succes- en faalfactoren voor innovatie. Het niet tijdig inspelen op het beschermen van publieke waarden, kan het vertrouwen van consumenten en burgers schaden en leiden tot falende innovaties en kostbare trajecten. Met het op een juiste manier borgen van publieke waarden in toekomstige ICT-innovaties kan Nederland een gidsland worden en kansen creëren voor het Nederlandse bedrijfsleven.

### *Actiepunten in het Digitaliseringsakkoord*

In een "Digitaliseringsakkoord" dienen verantwoordelijkheden van verschillende partijen te worden gedefinieerd en vastgelegd. Een belangrijk onderdeel van een dergelijk akkoord vormen de verantwoordelijkheden van bedrijven. ICT-ontwikkelaars dienen doordrongen te zijn van de maatschappelijke en ethische impact van hun producten, en dienen zich in te spannen voor het beschermen van mensenrechten en grondrechten. De verantwoordelijkheid van bedrijven om mensenrechten te respecteren, zijn onder andere opgenomen in de Richtlijnen voor Multinationale Ondernemingen van de OESO. Bedrijven dienen zich actief in te spannen om risico's op schendingen van mensenrechten door henzelf of partijen in hun keten te onderkennen, en waar mogelijk schendingen te voorkomen.

Via gedragscodes van brancheorganisaties kan praktische uitwerking worden gegeven aan deze internationale standaarden. Ze geven richting aan de omgang met maatschappelijke en ethische vragen. Leer van bestaande structuren en tools op het gebied van dataprotectie, zoals privacy impact assessments en privacy by design. Zo kan een *ethical impact assessment* bijvoorbeeld een middel zijn om maatschappelijke en ethische knelpunten anders dan privacy in een vroege fase van productontwikkeling zichtbaar te maken. De overheid kan hier een rol spelen door in haar onderzoeksfinanciering en innovatiebeleid nadrukkelijk ruimte te maken voor maatschappelijke en ethische implicaties van nieuwe technologie.

Daarnaast dient het Digitaliseringsakkoord aandacht te besteden aan het bevorderen van 'technologisch burgerschap' o.a. door het stimuleren van digitale vaardigheden. Dat kan concreet vorm krijgen door in het onderwijs mediawijsheid te verbreden, en ruimte te maken voor programmeren en andere digitale vaardigheden. Dat geldt niet alleen voor het basis- en voorgezet onderwijs voor de burgers van de toekomst, maar juist ook voor het onderwijs van de professionals van nu. Van de zorg tot aan het gerechtelijk systeem is het van belang dat professionals kennis nemen van de invloed van de nieuwe digitaliseringsgolf op publieke waarden.

Tot slot is het van belang dat het akkoord vastlegt hoe het tegengeluid van niet-gouvernementele organisaties (ngo's) en burgers beter kan worden ondersteund, bijvoorbeeld met zogenaamde class actions, of door de wenselijkheid van het opheffen van het verbod op grondwettelijke toetsing te onderzoeken.



#### **4. Versterken technologisch burgerschap middels een maatschappelijke dialoog**

Actiepunten:

- Overheid, bedrijven en maatschappelijk middenveld: ondersteun technologisch burgerschap door een nationale dialoog over nieuwe maatschappelijke en ethische digitaliseringsvraagstukken te organiseren.

De maatschappelijke discussie over de maatschappelijke en ethische betekenis van de nieuwe digitaliseringsgolf is vooralsnog beperkt, met name over de nieuwe vraagstukken als gelijke behandeling, menselijke waardigheid, autonomie en nieuwe machtsverhoudingen tussen bedrijven en consumenten, bedrijven en overheden, en tussen burgers en overheden. Dat betekent dat er een belangrijke taak ligt in het organiseren van een nationale dialoog over deze ontwikkelingen. De overheid dient hiertoe het startschot te geven, maar een maatschappelijke dialoog kan alleen succesvol zijn in samenwerking met het veld. De uitvoerende verantwoordelijkheid voor het organiseren van de dialoog zal niet bij de overheid liggen, maar zij is wel de initiator en aanjager. Er kan gebruik worden gemaakt van de ervaring die is opgedaan met de organisatie van eerdere dialogen, zoals de maatschappelijke dialoog nanotechnologie.

De dialoog vormt samen met het stimuleren van digitale vaardigheden (zie hierboven) de kern van technologisch burgerschap. Technologisch burgerschap houdt in dat burgers zich bewust zijn van de technologische cultuur waarin ze leven, en begrijpen op welke manier technologie invloed op hen uitoefent (Van Est 2016). Een 'technologisch burger' is geïnformeerd over de werking van technologie, kan kritisch nadenken over die werking en de betekenis daarvan voor zijn leefwereld, en kan op basis daarvan kiezen welke technologie hij wel of niet kan of wil gebruiken. Dat betekent bijvoorbeeld dat mensen begrijpen hoe profilering en zelflerende algoritmes werken en hoe dat hen beïnvloedt, en dat ze in staat zijn zich te verweren tegen ongewenste invloeden, en alternatieven kunnen kiezen. Technologisch burgerschap vraagt daarom om het vergroten van het maatschappelijk bewustzijn en het stimuleren van de meningsvorming over de invloed en betekenis van de nieuwe digitaliseringsgolf.

#### **5. Zorg voor periodieke politieke discussie in de Eerste en Tweede Kamer over de governance van maatschappelijke en ethische digitaliseringsvraagstukken.**

Actiepunten:

- Periodieke discussie over de governance van maatschappelijke en ethische digitaliseringsvraagstukken.

Een overkoepelende kabinetsvisie over de omgang met maatschappelijke en ethische betekenis van digitalisering brengt met zich mee dat het onderwerp ook periodiek op de politieke agenda komt te staan. Daarmee wordt invulling gegeven aan de geconstateerde behoefte in het parlement aan een structurele discussie over maatschappelijke en ethische digitaliseringsvraagstukken. Die behoefte blijkt uit oproepen vanuit het parlement, waarbij de Eerste en Tweede Kamer de regering regelmatig verzoeken om een integrale visie te vormen op gebieden als privacy, of de rol van ethiek in innovatiebeleid. De motie Gerkens (zie kader 6.1) en de motie Ester c.s. (Kamerstukken I, 2013-2014, 33750 XIII) zijn daar voorbeelden van. Motie Ester verzoekt het Ministerie van Economische

Zaken om jaarlijks te rapporteren over de rol van ethiek in het innovatiebeleid, en probeert daarover een structureel terugkerende politiek-ethisch debat in de Eerste Kamer mogelijk te maken. Tot nu toe wordt het politieke debat met name gedreven door incidenten. Door het onderwerp periodiek (liefst commissieoverstijgend) op de Kameragenda te zetten ontstijgt het debat het huidige gefragmentariseerde en incidentele karakter, en kan worden gezien of de ondernomen acties om het governancelandschap te versterken ook daadwerkelijk vruchten hebben afgeworpen: is het landschap voldoende versterkt? Zijn er nieuwe blinde vlekken ontstaan? En zijn er aanvullende acties gewenst?

# Inhoudsopgave

Voorwoord	6
Samenvatting	7
1 Inleiding	20
1.1 De motie Gerkens	20
1.2 De context van de motie	20
1.3 Onderzoeksvragen en aanpak	21
1.4 Leeswijzer	24
2 De nieuwe digitale golf	26
2.1 Inleiding	26
2.2 Middelen om te digitaliseren	27
2.3 Objecten van digitalisering	30
2.4 De digitale wereld	41
2.5 De vier werelden bijeen: een nieuwe fase in de digitale samenleving	43
2.6 Tot slot	45
3 Maatschappelijke en ethische issues van digitalisering	46
3.1 Inleiding	46
3.2 Materiële wereld	48
3.3 Biologische wereld	57
3.4 Socio-culturele wereld	63
3.5 Digitale wereld	69
3.6 Conclusie	74
4 Governance in historisch perspectief	79
4.1 Inleiding	79
4.2 Jaren 1970: maatschappelijke en ethische zorgen over wetenschap en technologie	81
4.3 Jaren 1980: institutionalisering van maatschappelijke en ethische omgang met wetenschap en technologie	82
4.4 Jaren 1990: vermaatschappelijking en regulering van de bio-ethiek	84
4.5 Jaren 2000: onderzoek, signalering en debat over ethiek en bio- en nanotechnologie	88
4.6 Jaren 2010: behoefte aan reflectie op en debat over maatschappelijke en ethische aspecten van innovatie	92
4.7 Noodzaak voor een breed perspectief op het governance-ecosysteem	92
4.8 Raamwerk voor het governance-ecosysteem	95
4.9 Tot slot: Langetermijndynamiek van het governance-ecosysteem	100

5	Blinde vlekken in het governancelandschap	102
5.1	Inleiding	102
5.2	Rol van de wetenschap	103
5.3	Rol van grond- en mensenrechten	104
5.4	Rol van maatschappelijke actoren	107
5.5	Agendavorming	111
5.6	Beleidsvorming en -bepaling	114
5.7	Beleidsuitvoering	118
5.8	Conclusie	120
6	Conclusie: Borgen van publieke waarden in de digitale samenleving	125
6.1	Inleiding	125
6.2	Een nieuwe digitale golf: digitalisering als cybernetisering	126
6.3	Publieke waarden in het geding	128
6.4	Lessen uit het verleden	129
6.5	Blinde vlekken in het governancelandschap voor ethische en maatschappelijke digitaliseringsvraagstukken	130
6.6	Opwaarderen: een actieprogramma voor een verantwoorde digitale samenleving	132
6.7	Tot slot	139
	Bibliografie	141
	Appendix A: Uitgebreide analyse governance-ecosysteem	155
	Inleiding	155
	Grond- en mensenrechten	156
	Wetenschap	160
	Maatschappelijke actoren en debat	163
	Agendavorming	171
	Beleidsvorming en -bepaling	177
	Beleidsuitvoering	190
	Bibliografie	196
	Appendix B: De betekenis van publieke governance	203
	Governance als maatschappelijke sturing	203
	Governance van publieke vraagstukken	203
	Governance als de vormgeving van interactie tussen overheid en maatschappij	204
	Meta-governance van het governance-ecosysteem	205
	Relevante vragen vanuit governanceperspectief	205
	Bibliografie	207
	Appendix C: Geraadpleegde experts	208
	Over de auteurs	209

# 1 Inleiding

## 1.1 De motie Gerkens

Met de motie Gerkens c.s. van 23 september 2014 verzocht de Eerste Kamer de regering 'het Rathenau Instituut te vragen een onderzoek te doen naar de wenselijkheid van een commissie die kan adviseren over de ethische kant van de digitalisering van de samenleving' (zie Kader 1). De motie werd ingediend door de SP, en ondertekend door D66, VVD, CDA, GroenLinks en de PvdA. Zoals verzocht in de motie Gerkens heeft het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) het Rathenau Instituut gevraagd onderzoek te doen naar de vraag die in de motie wordt gesteld. Naar aanleiding van deze motie brengt het Rathenau Instituut deze studie uit, waarin het maatschappelijke en ethische vragen omtrent de digitalisering van de samenleving in kaart brengt en onderzoekt in hoeverre de signalering en monitoring van die vragen ook institutioneel verankerd is.

### **Kader 1.1 Motie van het lid Gerkens c.s. voorgesteld op 23 september 2014**

De Kamer, gehoord de beraadslagingen, constaterende, dat de digitale technologie met *the Internet of Things* alles en iedereen met elkaar zal verbinden; constaterende, dat deze niet te stuiten ontwikkeling kansen zal bieden voor de maatschappij, maar ook bedreigingen; overwegende, dat de effecten van deze digitale ontwikkeling op de maatschappij niet alleen een technologische, maar ook een maatschappelijke, sociaal juridische en sociaal psychologische is; verzoekt de regering het Rathenau Instituut te vragen een onderzoek te doen naar de wenselijkheid van een commissie die kan adviseren over de ethische kant van de digitalisering van de samenleving, en gaat over tot de orde van de dag.

Ondertekend door Eerste Kamerleden Gerkens, Franken, K.G. de Vries, Strik, Duthler, Van Boxtel.

## 1.2 De context van de motie

De motie Gerkens c.s. werd ingediend tijdens een debat in de Eerste Kamer over privacy en toezicht op de inlichtingen- en veiligheidsdiensten in september 2014. Het debat vond plaats ongeveer een jaar nadat de NRC berichtte over via Edward Snowden verkregen documenten over de werkwijze van de Nederlandse inlichtingendiensten.<sup>1</sup> Tegelijk verwijst de motie naar het Internet

---

<sup>1</sup> Op 30 november 2013 berichtte NRC over een intern NSA-verslag waaruit zou blijken dat de AIVD inbrak op servers van internetfora en daarbij de gegevens van alle deelnemers onderschepte. NRC.nl: AIVD hackt internetfora, 'tegen wet in', 30 november 2013

of Things en de bredere maatschappelijke, sociaal juridische en sociaal psychologische effecten van de ontwikkeling van digitalisering.

De vraag in de motie naar een commissie vatten we op als een meta-vraag (zie paragraaf 1.3 Onderzoeksvragen en aanpak). Er spreekt een zorg uit of de huidige institutionele en wettelijke kaders en vormen van toezicht voldoende zijn uitgerust om de uitdagingen van de digitaliserende samenleving het hoofd te bieden. Deze achterliggende zorg is leidend bij de aanpak van deze studie en de conclusies van dit rapport.

De motie verzoekt de regering om het Rathenau Instituut onderzoek te laten doen naar de ethische aspecten van digitalisering. De vraag in de motie sluit aan bij de taakstelling van het Rathenau Instituut en haar inhoudelijke expertise. Al dertig jaar brengt het Rathenau Instituut de ethische en maatschappelijke betekenis van automatisering – later spreekt men van digitalisering – in kaart.<sup>2</sup> Het Rathenau Instituut heeft expliciet de taak dit te doen voor het parlement, om zo politieke oordeelsvorming mogelijk te maken.<sup>3</sup> Voor het Rathenau Instituut is digitalisering de laatste jaren een zeer belangrijk thema geweest dat op talloze wijzen is geagendeerd. Er zijn verschillende ontwikkelingen aan de orde gekomen, zoals het Internet of Things, robotica, biometrie, slimme mobiliteit, big data, digitale platformen, en digitalisering in de gezondheidszorg, verzekeringswereld en het boerenbedrijf.<sup>4</sup> De vraag in de motie brengt dus een groot deel van het onderzoek van het Rathenau Instituut van de afgelopen jaren samen.

### 1.3 Onderzoeksvragen en aanpak

De centrale vraag van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties is: in hoeverre het wenselijk is om een commissie in te stellen die kan adviseren over de ethische kant van de digitalisering van de samenleving? Om deze vraag te kunnen beantwoorden, stellen we de verschillende deelvragen op. Ze hebben betrekking op digitalisering, ethische en maatschappelijke kwesties en de *governance* van die kwesties. In deze paragraaf lichten we per onderzoeksvraag onze aanpak toe.

---

<sup>2</sup> Het instituut komt voort uit de 'commissie Rathenau' die in 1979 de regering moest adviseren over de maatschappelijke gevolgen van automatisering. De commissie, voorgezeten door Gerhart Rathenau, voormalig directeur van het Natlab van Philips, adviseerde om de gevolgen van nieuwe technologie voortaan systematisch in kaart te brengen. Aan die aanbeveling werd gehoor gegeven met de oprichting van NOTA, de Nederlandse Organisatie voor Technologisch Aspectenonderzoek, later omgedoopt tot Rathenau Instituut.

<sup>3</sup> Zie het instellingsbesluit, [wetten.overheid.nl/BWBR0026157/2009-07-24](http://wetten.overheid.nl/BWBR0026157/2009-07-24), 24 juli 2009, waarin staat: '*Het instituut heeft als taak bij te dragen aan het maatschappelijke debat en de politieke oordeelsvorming over vraagstukken die samenhangen met of het gevolg zijn van wetenschappelijke en of technologische ontwikkelingen waaronder de ethische, de maatschappelijke, de culturele en de wettelijke aspecten daarvan. Het instituut levert in het bijzonder bijdragen aan de politieke oordeelsvorming in de beide Kamers van de Staten-Generaal en in het Europese parlement.*'

<sup>4</sup> Het Instituut doet dat onder andere door context te bieden en beleidsopties te presenteren.

Zie o.a. Beyond control: Consumer privacy in the Internet of Things (2016), Digitalisering van dieren (2016), De meetbare mens (2016), De robotsamenleving (2015), Verzekeren in de data-gedreven samenleving (2015), Dicht op de huid (2015), De data-gedreven samenleving (2015), Eerlijk advies (2014), De Kracht van platformen (2014), Tem de robotauto (2014), Intieme technologie (2014), Op advies van de auto (2013), Voorgeprogrammeerd (2012), Overall robots (2012), Check-in, check-out (2010), Databases (2010), Het glazen lichaam (2008), Van privacyparadijs tot controlestaat (2007).

**Digitalisering:**

De motie spreekt van de *digitalisering van de samenleving*. De eerste stap van dit onderzoek is daarom om meer inzicht te krijgen in wat die digitalisering behelst. Dit doen we middels twee onderzoeksvragen:

- Welke relevante technologische ontwikkelingen ondersteunen het proces van digitalisering van de samenleving?
- En op welke wijze zal de digitalisering van de samenleving de komende tien tot vijftien jaar onder invloed van nieuwe technologieën mogelijk vorm krijgen?

Op basis van literatuuronderzoek schetsen we hoe digitalisering in de afgelopen zes decennia vorm heeft gekregen. We laten zien hoe steeds meer aspecten van de ‘analoge’ maatschappij digitaliseren. We beschrijven dit aan de hand van drie werelden: de materiële wereld, de biologische wereld en de socio-culturele wereld. Vervolgens beschrijven we de groeiende ‘digitale wereld’. Per wereld selecteren we twee technologiegebieden (acht in totaal) waarvan we verwachten dat ze de komende tien tot vijftien jaar vormgeven aan de digitaliserende samenleving: robotica, biometrie, persuasieve technologie, digitale platformen, augmented reality, virtual reality en sociale media, kunstmatige intelligentie en algoritmen en big data. We kiezen deze acht gebieden omdat ze de reikwijdte van de impact van de nieuwe digitaliseringsgolf weergeven. De technologiegebieden vormen het uitgangspunt voor de volgende deelvraag.

**Ethische en maatschappelijke kwesties:**

Als duidelijk is welke technologiegebieden de komende jaren de digitale samenleving zullen vormgeven, kunnen we onderzoeken welke ethische en maatschappelijke vragen deze technologieën oproepen. De volgende deelvraag luidt dan ook:

- Welke maatschappelijke en ethische kwesties roept de digitaliserende samenleving op?

We spreken hier over ethische en maatschappelijke vraagstukken. De motie Gerkens spreekt over de *ethische* kanten van de digitaliserende samenleving. In de toelichtende tekst (zie kader 1) wordt duidelijker wat de Eerste Kamer daarmee voor ogen heeft: de toelichting spreekt over ‘maatschappelijke, sociaal juridische en sociaal psychologische’ effecten van digitale ontwikkelingen. Uit deze toelichting spreekt een brede opvatting van ethiek. Daarom benaderen we ethiek in deze studie ook breed. We definiëren ethiek in deze studie als de systematische reflectie op moraal, oftewel het geheel van normen en waarden dat feitelijk bestaat in een samenleving. We bezien ethiek dus niet als iets dat alleen op individueel niveau speelt, maar ook op maatschappelijk niveau. Daarom zullen we in deze studie steeds kijken naar ethische én maatschappelijke kwesties die de digitaliserende samenleving oproept. We brengen deze in kaart op basis van een uitgebreide studie van de wetenschappelijke literatuur daarover. We laten per technologiegebied zien welke kwesties daar spelen en hoe ze zich manifesteren.

**Governance:**

De motie vraagt naar de wenselijkheid van een commissie die kan adviseren over de ethische aspecten van de digitaliserende samenleving. Zoals hierboven genoemd, duidt die vraag op een achterliggende zorg in de Eerste Kamer of de huidige wettelijke kaders, toezichtsarrangementen en maatschappelijke weerbaarheid nog voldoende zijn om opkomende ethische en maatschappelijke

kwesties rondom digitalisering het hoofd te bieden. In deze studie bezien we de vraag in de motie dan ook vanuit deze achterliggende vraag.

We onderzoeken hoe de *governance* van ethische en maatschappelijke kwesties in de digitaliserende samenleving vorm krijgt en of die adequaat is. We willen zicht krijgen op welke kwesties bestaande instituties wel of niet oppakken, op welke manier: zijn er blinde vlekken ten aanzien van de omgang met (nieuwe) ethische en maatschappelijke kwesties? De vervolgvraag is welke rol een commissie zou kunnen spelen. We dienen daarom ook inzicht te krijgen in wat voor soort commissies er bestaan rondom ethische en maatschappelijke kwesties van technologie en hoe we de rol van een commissie kunnen begrijpen.

De laatste deelvragen luiden daarom:

- Hoe kunnen we de governance van maatschappelijke en ethische kwesties van technologische ontwikkelingen begrijpen, en welke rol spelen commissies daarbij?
- Hoe krijgt de governance van maatschappelijke en ethische kwesties van de digitaliserende samenleving op dit moment vorm? Welke kwesties worden goed of minder goed opgepakt en zijn er blinde vlekken te identificeren?
- Welke rol kan een commissie spelen in het brede governance-ecosysteem van de digitaliserende samenleving?

Governance is een meerduidig concept. In Appendix B introduceren we een aantal inzichten en begrippen uit de literatuur die behulpzaam zijn bij het nadenken over de governance van de maatschappelijke en ethische aspecten van wetenschap en technologie. Voor onze aanpak is het van belang dat we een onderscheid maken tussen de *governance* en *meta-governance* van ethische en maatschappelijke problemen.

Governance betreft kort gezegd het collectief besturen van maatschappelijke problemen in onze samenleving (voor een uitgebreide definitie zie Appendix B). Het draait om vragen als:

- Welke publieke problemen zijn gesignaleerd en politiek geagendeerd?
- Welke belangen of waarden zijn goed of minder goed gearticuleerd?
- Hoe discussiëren diverse actoren in de samenleving over deze problemen?
- Wie is daarbij wel of niet en meer of minder betrokken?

Meta-governance geeft aan dat de collectieve besturing van publieke problemen plaatsvindt in een *governance-ecosysteem*, oftewel in een verzameling van instituties, bestuurlijke en maatschappelijke processen en actoren. Meta-governance geeft de opbouw, structuur en werking van het governance-ecosysteem weer en draait om vragen als:

- Welke instituties zijn er om te discussiëren over publieke problemen en deze politiek aan te kaarten?
- Op welke manieren vindt afstemming plaats tussen publieke en private actoren?
- Op welke wijze worden publieke waarden institutioneel geborgd?
- Welke instituties zijn er door de jaren heen opgebouwd om dat te doen?

In deze studie willen we zicht krijgen op de governance en de meta-governance van maatschappelijke en ethische kwesties die ontstaan door digitalisering. Dat doen we op twee



manieren. Allereerst kijken we hoe we in algemene zin het governance-ecosysteem in Nederland ten aanzien van maatschappelijke en ethische kwesties van technologie kunnen begrijpen. Hiervoor stellen we een algemeen conceptueel raamwerk op, gebaseerd op een overzicht van governancemechanismen die in Nederland de afgelopen halve eeuw zijn ontstaan op vier technologische gebieden: biotechnologie, ICT, mensgebonden onderzoek en dierexperimenten. Dit historisch overzicht maakt ook duidelijk wat voor soort commissies in het verleden zijn ingesteld rondom ethische en maatschappelijke kwesties op deze terreinen, en welke rol zij vervulden binnen het governance-ecosysteem.

Vervolgens gebruiken we het algemene conceptuele raamwerk om zicht te krijgen op de manier waarop het governance-ecosysteem van ethische en maatschappelijke kwesties rondom digitalisering vorm krijgt. Via deskresearch brengen we in kaart welke partijen deel uitmaken van het ecosysteem, welke publieke problemen zij signaleren (en welke niet), in hoeverre deze problemen politiek zijn geagendeerd, en hoe beleidsmatig om wordt gegaan met de gesignaleerde problemen. We hebben in deze analyse gekeken naar activiteiten tot oktober 2016. Op basis daarvan kunnen we concluderen waar mogelijk blinde vlekken liggen in het huidige governance-ecosysteem en welke rol een commissie zou kunnen spelen.

We merken op dat het Rathenau Instituut onderdeel is van het governance-ecosysteem rondom maatschappelijke en ethische kwesties van technologie en van digitalisering. Zoals hierboven vermeld heeft het Rathenau Instituut als expliciete taak publieke en politieke meningsvorming over wetenschap en technologie te stimuleren. In de analyse van het ecosysteem benoemen we daarom ook de activiteiten van het Rathenau Instituut.

Naast literatuuronderzoek en deskresearch hebben we voor dit onderzoek gesprekken gevoerd met diverse deskundigen en betrokkenen (zie Appendix C voor het overzicht van geraadpleegde experts). De bevindingen van deze studie zijn daarnaast voorgelegd en besproken met een begeleidingscommissie, bestaande uit zes mensen met wetenschappelijk en politiek-bestuurlijke ervaring (zie Appendix C). Het Rathenau Instituut is verantwoordelijk voor de bevindingen in dit rapport. Tot slot is dit rapport, volgens de kwaliteitsprocedures van het Rathenau Instituut, intern ter review voorgelegd.

## **1.4 Leeswijzer**

De onderzoeksvragen met betrekking tot digitalisering, maatschappelijke en ethische aspecten en governance werken we in de volgende hoofdstukken stapsgewijs verder uit.

Hoofdstuk 2 beschrijft hoe digitalisering de afgelopen halve eeuw is verlopen en welke technologiegebieden naar verwachting de komende jaren van invloed zullen zijn op de digitale samenleving. Deze technologiegebieden zorgen voor een nieuwe technologische golf en luiden een nieuwe fase van de digitale samenleving in. Waar digitalisering aanvankelijk bestond uit het op grote schaal verzamelen van gegevens over de materiële, biologische en sociale wereld, richt digitalisering zich nu op de grootschalige analyse én toepassing van die gegevens. Dat maakt real-time interventies en (bij)sturing mogelijk. Denk bijvoorbeeld aan de nieuwsfeeds van sociale

mediagebruikers, die sociale mediabedrijven real-time 'op maat' aanpassen, op basis van de verzameling en analyse van het surfgedrag van diezelfde sociale mediagebruikers. Deze *cybernetische loop* is kenmerkend voor de huidige fase van digitalisering.

Hoofdstuk 3 brengt in kaart welke maatschappelijke en ethische kwesties de nieuwe technologische golf momenteel oproept. We bespreken per technologiegebied de meest urgente kwesties en illustreren deze aan de hand van actuele voorbeelden. Duidelijk wordt dat maatschappelijke en ethische kwesties rondom digitalisering niet alleen betrekking hebben op privacy en veiligheid, maar nieuwe fundamentele vragen oproepen met betrekking tot onder andere rechtvaardigheid, gelijke behandeling, autonomie en menselijke waardigheid. Wie heeft bijvoorbeeld zicht op welke keuzes de software van sociale mediabedrijven maakt om bepaalde nieuwsberichten wel of niet te tonen? Welke taken willen we overlaten aan robots, en welke niet?

Hoofdstuk 4 laat zien hoe we het governance-ecosysteem ten aanzien van maatschappelijke en ethische kwesties van technologie kunnen begrijpen. Het hoofdstuk blikt circa een halve eeuw terug op hoe we in Nederland zijn omgegaan met ethische en maatschappelijke kwesties rondom biotechnologie, ICT, mensgebonden onderzoek en dierexperimenten. Het overzicht laat zien welke commissies er zijn geweest op deze gebieden en wat voor type commissies dat waren. Aan de hand van het historisch overzicht stellen we een algemeen conceptueel raamwerk op hoe het governance-ecosysteem in Nederland ten aanzien van maatschappelijke en ethische kwesties van technologie eruit ziet. Daarin onderscheiden we vier domeinen: grond- en mensenrechten, wetenschap, maatschappij en politiek en bestuur.

In hoofdstuk 5 gebruiken we het conceptueel raamwerk om zicht te krijgen op de wijze waarop het governance-ecosysteem van ethische en maatschappelijke kwesties rondom digitalisering momenteel vorm krijgt. De analyse richt zich op Nederland, maar benoemt ook enkele relevante ontwikkelingen in het buitenland. Op basis van deskresearch brengen we in kaart welke activiteiten diverse organisaties en actoren voorstellen, voorbereiden, initiëren of uitvoeren om in te spelen op de maatschappelijke en ethische uitdagingen rondom digitalisering. We zetten ook op een rij welke commissies er op dit terrein reeds zijn of welke commissies door diverse organisaties zijn voorgesteld. Op verschillende plekken in het governancelandschap identificeren we blinde vlekken.

Hoofdstuk 6 bevat de conclusie van de studie. We blikken kort terug op de deelvragen en vatten de belangrijkste bevindingen van deze studie samen. We concluderen dat de verregerende digitalisering van de maatschappij fundamentele ethische en maatschappelijke vraagstukken oproept. Overheid en samenleving zijn op dit moment niet adequaat uitgerust om met deze thematiek om te gaan. Om publieke waarden en grondrechten in het digitale tijdperk nu en in de toekomst te kunnen borgen vraagt om een upgrade, of opwaardering, van het governancesysteem. Deze opwaardering vereist dat alle partijen – overheid, bedrijfsleven en maatschappelijk middenveld – nu in actie komen om digitalisering in goede banen te leiden. We stellen daarom een actieprogramma voor om op een verantwoorde manier vorm te geven aan de digitale samenleving.

## 2 De nieuwe digitale golf

### 2.1 Inleiding

Dit hoofdstuk beschrijft hoe we de voortdurende digitalisering van de samenleving kunnen begrijpen. Wat is er de afgelopen zes decennia gedigitaliseerd, wat zijn de effecten van die digitalisering, en hoe ziet de toekomstige digitale samenleving eruit? We trachten niet om een volledig beeld te schetsen van alles dat digitaliseert, maar de lezer een gevoel te geven van wat digitalisering inhoudt. We kijken daarbij zowel naar het verleden (welke relevante technologische ontwikkelingen hebben het proces van digitalisering ondersteund) als naar de toekomst (welke relevante technologische ontwikkelingen geven de komende vijf tot tien jaar de digitale samenleving vorm?). Dit laatste levert een selectie op van acht technologiegebieden op. In het volgende hoofdstuk vormen deze gebieden het uitgangspunt voor de analyse van ethische en maatschappelijke kwesties die de digitale samenleving oproept.

We beginnen dit hoofdstuk met een beknopt historisch overzicht van ontwikkelingen in de micro-elektronica en de telecommunicatie: belangrijke technieken, of *middelen*, om te digitaliseren (paragraaf 2.2). Dan laten we zien hoe steeds meer gebieden uit de ‘analoge’ maatschappij digitaliseren. We onderscheiden daarbij drie ‘werelden’ die het *object* van digitalisering zijn: de materiële wereld, de biologische wereld, en de socio-culturele wereld (paragraaf 2.3). Voor iedere wereld beschrijven we belangrijke mijlpalen van digitalisering. Vervolgens beschrijven we de almaar uitdijende digitale wereld (paragraaf 2.4). Per wereld selecteren we twee technologiegebieden voor de analyse van maatschappelijke en ethische kwesties. In paragraaf 2.5 brengen we de vier werelden bijeen: welke nieuwe fase in de ontwikkeling van de digitaliserende samenleving is waar te nemen? Tot slot vatten we in paragraaf 2.6 de belangrijkste bevindingen uit dit hoofdstuk samen.

#### Kader 2.1 Digitalisering

Digitaliseren betekent letterlijk ‘[informatie, red] omzetten in digitale vorm ([in, red] nullen en enen)’ (Van Dale). Denk bijvoorbeeld aan een VHS-videoband die in digitale vorm wordt omgezet en zo is af te spelen op een computer. Of aan een foto die wordt gescand en door de computer vertaald wordt in pixels. Anno 2016 kennen we steeds meer digitale producten en diensten, zoals digitale muziek, streamingdiensten of de digitale bankrekening.

Inmiddels is duidelijk dat digitalisering niet slechts het omzetten van een analogo proces in bits en bytes behelst. Met het omzetten van informatie in digitale vorm krijgt namelijk informatie ook andere eigenschappen, en zijn er nieuwe dingen mogelijk. In 1995 schreef Nicholas Negroponte *Being Digital* waarin hij aangaf dat digitalisering informatie makkelijker te transporteren, manipuleren en te integreren is. Rond die tijd gaan diverse wetenschappers, waaronder Manuel Castells in zijn klassieker *The Rise of the Network*

*Society* digitalisering (het netwerk) zien als dé dominante organisatiestructuur voor de samenleving die bestaande manieren van productie, ervaring, macht en cultuur zal veranderen (Castells 1995; Van Dijk 1997). Tien jaar later beschreef Benkler (2006) in *The Wealth of Networks* hoe informatietechnologie nieuwe vormen van samenwerking mogelijk maakt met fundamentele veranderingen voor economie en maatschappij als gevolg.

ICT, en de daaruit voortvloeiende digitalisering, wordt – net zoals stoom of elektriciteit – op ontelbare manieren ingezet. Daarom spreekt men ook wel van een generieke technologie (*general purpose technology*) (Bresnahan & Trajtenberg 1995). Die technologie maakt niet alleen vele nieuwe producten mogelijk, maar heeft op den duur invloed op tal van maatschappelijke processen.

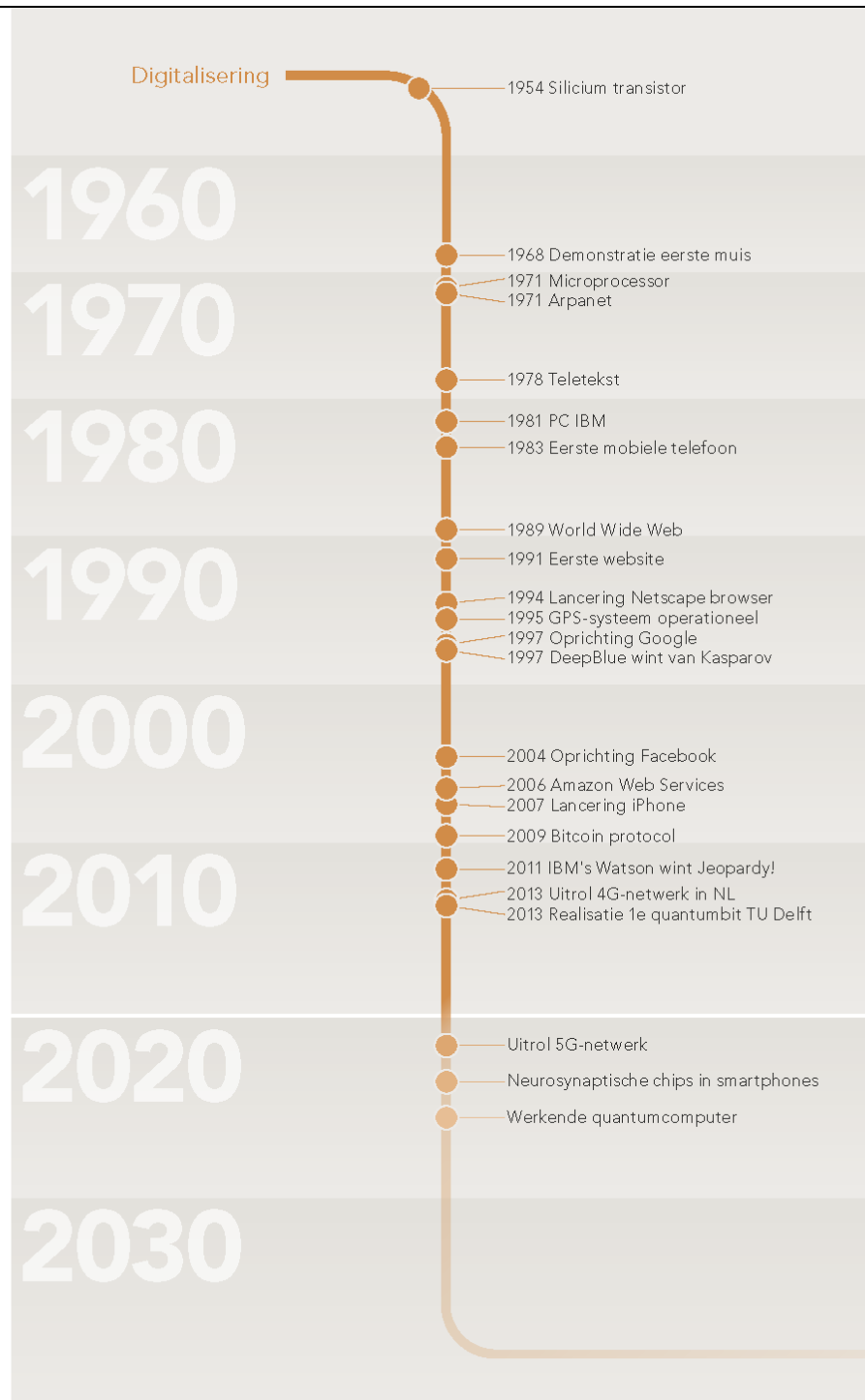
De invloed van informatietechnologie en digitalisering op de samenleving wordt alom herkend. Maar de manier waarop de digitale samenleving vorm krijgt, wordt niet uitsluitend wordt bepaald door (digitale) technologie. Samenleving en technologie beïnvloeden elkaar op complexe wijze. In deze studie gaan we ervan uit dat maatschappelijke, economische, politieke en technologische processen elkaar wederzijds beïnvloeden (Misa et al. 2003). Dat betekent dat, hoewel we ons hier beperken tot een beschrijving van de technologische ontwikkelingen, we ervanuit gaan dat de verdere ontwikkeling van de digitaliserende samenleving wordt beïnvloed door bestaande normen, regels, instituties, infrastructuur, en dat digitale technologie op haar beurt diezelfde normen, regels, instituties en infrastructuur beïnvloedt.

## 2.2 Middelen om te digitaliseren<sup>5</sup>

In deze paragraaf beschrijven we hoe digitalisering de afgelopen halve eeuw heeft vorm gekregen. We besteden daarbij aandacht aan de achterliggende techniek die digitalisering mogelijk maakt. Dat zijn bijvoorbeeld apparatuur (hardware), software, en telecommunicatie en infrastructuur; kortom informatie- en communicatietechnologie (ICT). Dit doen we door middel van een beknopt historisch overzicht van ontwikkelingen in de micro-elektronica en telecommunicatie (zie figuur 2.1). In kader 2.1 geven we kort verschillende positioneringen en conceptualisering van het begrip digitalisering weer, om aan te geven dat digitalisering niet slechts een instrumentele verandering behelst, maar er met digitalisering fundamentele veranderingen in economie en maatschappij plaatsvinden.

---

<sup>5</sup> Deze paragraaf biedt een beknopt historisch overzicht van ontwikkelingen in de micro-elektronica en telecommunicatie. Voor uitgebreide overzichtswerken zie bijvoorbeeld Van den Bogaard et al. (2008): *De eeuw van de computer: de geschiedenis van de informatietechnologie in Nederland*.

**Figuur 2.1** Overzicht middelen voor digitalisering

Rathenau Instituut

In de jaren veertig en vijftig legden doorbraken in de micro-elektronica en de telecommunicatie een belangrijke technologische basis voor digitalisering. Die doorbraken waren onder meer de eerste programmeerbare computer (1941) en de eerste op silicium gebaseerde transistor (1954). Een transistor dient om elektronische signalen mee te versterken of te schakelen. De transistor is de fundamentele bouwsteen van iedere chip, en staat daarmee aan de basis van iedere ICT-

toepassing. De afgelopen vijftig jaar verdubbelde het aantal transistors op een chip ongeveer iedere anderhalf tot twee jaar. Deze trend van miniaturisering en het tempo waarin de innovatie plaatsvindt, wordt de Wet van Moore genoemd, en heeft de afgelopen zes decennia geleid tot steeds kleinere, krachtigere en betaalbaardere computers.<sup>6</sup>

De eerste computers in de jaren vijftig waren enorme kolossen en werden vooral gebruikt door defensie en in de wetenschap voor ingewikkelde rekentaken. Ook banken begonnen deze 'mainframe computers' te gebruiken. In de jaren zestig werden de computers stapsgewijs kleiner en deed de 'minicomputer' – zo groot als een koelkast – zijn intrede. Een doorbraak kwam in 1971 met de microprocessor van Intel. Deze was slechts enkele millimeters groot, maar even krachtig als hun reusachtige neven uit de jaren vijftig. Zo konden de toen nog kleine bedrijfjes Apple en Microsoft nog kleinere computers ontwerpen die los van een mainframe op een bureau konden staan. Maar pas in de jaren tachtig deed informatietechnologie op brede schaal zijn intrede in de maatschappij, met de komst van de Personal Computer (PC) van IBM. Al snel deed de PC op vele werkvloeren zijn intrede, met tekstverwerking en spreadsheet als de belangrijkste toepassingen, en in de jaren daarna ook bij gezinnen thuis.

In de jaren negentig volgde de opkomst van mobiele telefonie en het internet. Ook begint in deze periode de digitalisering en convergentie van bestaande infrastructuren, zoals de kabel en de ether voor diensten als telefonie, radio en tv. De gevolgen van dit digitaliseringsproces zijn al snel overal merkbaar: in de zakelijke dienstverlening – de muziekhandel, de reisbranche, de logistiek, de detailhandel – en in semipublieke sectoren als het onderwijs, mobiliteit en de zorg. De groeiende beschikbaarheid van internet wereldwijd versterkt globalisering. Dat maakt het *outsourcen*, *offshoren* en automatiseren mogelijk van aanvankelijk productiewerk en later ook kenniswerk (Van Est & Kool 2015).

Na de eeuwwisseling ontwikkelde het internet zich van een passief, informatie gevend medium (web 1.0) naar een interactief medium waaraan gebruikers op allerlei manieren kunnen bijdragen (web 2.0): via het geven van reacties, eigen content plaatsen en het *taggen* en beoordelen van content van anderen. Het web wordt een 'platform voor datamanagement', vooral door de inzet van de verbondenheid en collectieve intelligentie van gebruikers (O'Reilly 2005). Sociale netwerksites als MySpace, Hyves en Facebook komen op, en andere sociale media zoals YouTube en Twitter. Met de opkomst van smartphones en andere mobiele apparaten als tablets, samen met de verdere ontwikkeling van snelle, draadloze internetverbindingen en *cloud*toepassingen, zijn het internet en de bijbehorende online diensten inmiddels niet meer weg te denken uit de economie en maatschappij.

---

<sup>6</sup> De Wet van Moore is gebaseerd op een voorspelling uit 1965 van Gordon Moore. Hij voorspelde dat het aantal transistors op een microchip, en daarmee de rekenkracht van computers, elke twee jaar zou verdubbelen, terwijl de kosten gelijk zouden blijven. Vijftig jaar later blijkt deze voorspelling nog steeds op te gaan. Er bestaat discussie hoe lang de Wet van Moore nog stand houdt. De verwachting is dat chips als ze circa vijf nanometer groot zijn hun fysieke grens hebben bereikt. Daarna stappen fabrikanten wellicht over naar 3D-chips (gestapelde chips). Een volgende stap zijn chips die niet meer gebaseerd zijn op siliconen, maar op optische, nano of biologische principes. IBM presenteerde bijvoorbeeld in 2015 een neurosynaptische chip, TrueNorth.

In de jaren na 2010 zien we de uitrol van 4G-netwerken, de opkomst van het Internet of Things (zie paragraaf 2.3) en steeds meer online toepassingen die gebruikmaken van een vorm van kunstmatige intelligentie, zoals spraakherkenning of betere zoekfunctionaliteit. In 2011 wint de supercomputer van IBM voor het eerst het tv-spelletje Jeopardy! en in 2016 wint Google's AlphaGo het zeer complexe spel Go van een menselijke expert.<sup>7</sup> Voor 2020 en de jaren daarna is de verwachting dat het 5G-netwerk wordt uitgerold, er nieuwe soorten snellere chips komen en er doorbraken ontstaan op het gebied van quantum computing.<sup>8</sup> In figuur 2.1 hebben we deze verwachtingen als onzekere toekomstige mijlpalen opgenomen.

## 2.3 Objecten van digitalisering

ICT en digitalisering is anno 2016 alomtegenwoordig in onze samenleving. Daarbij maakt ICT ook verbinding met andere technologiegebieden, zoals nanotechnologie, biotechnologie en neurotechnologie. Deze zogenoemde NBIC-convergentie is sinds eind jaren negentig steeds duidelijker zichtbaar. Digitalisering dringt zo door tot ieder aspect van ons leven: technologie nestelt zich *in* ons (bijvoorbeeld via hersenimplantaten), *tussen* ons (via sociale media als Facebook), weet steeds meer *over* ons (via big data en technieken als emotieherkenning), en weet zich steeds beter te gedragen *als* ons (robots en software vertonen intelligent gedrag en kunnen emoties nabootsen). Het Rathenau Instituut spreekt daarom in 2014 van de intiem-technologische revolutie (Van Est 2014).

De verwevenheid van ICT met andere technologieën maakt duidelijk dat allerlei verschillende aspecten uit ons leven digitaliseren. In dit hoofdstuk kunnen we echter niet al deze aspecten uitputtend behandelen. We maken daarom onderscheid tussen drie 'werelden':

1. de *materiële wereld* (zoals het productieproces, de openbare ruimte en ons huis);
2. de *biologische wereld* (zoals het menselijk lichaam, het brein en ons gedrag);
3. de *socio-culturele wereld* (zoals communicatie, culturele producten en organisaties)

We beschrijven voor iedere wereld belangrijke mijlpalen van digitalisering, en nog te verwachten technologische innovaties in 2020 en 2030 (zie figuur 2.2). Op basis daarvan selecteren we per wereld steeds twee technologiegebieden die de digitale samenleving naar verwachting de komende vijf à tien jaar vorm zullen geven. De werelden krijgen allemaal een virtuele representatie in de digitale wereld. Deze groeiende digitale wereld beschrijven we in paragraaf 2.4.

Het onderscheid tussen de drie werelden is een conceptueel onderscheid. In de praktijk zijn ze sterk verweven met elkaar, en overlappen ze elkaar. We beschrijven de werelden daarom steeds met een focus op *het object van digitalisering*. Dat betekent bijvoorbeeld dat we digitalisering van muziek behandelen in de socio-culturele wereld; we kijken naar muziek als cultureel product, als object van digitalisering. Dat neemt niet weg dat muziek fysieke dragers en instrumenten kent, en een fysiek productie- en distributieproces. Muziek heeft dus ook een plaats in de materiële wereld.

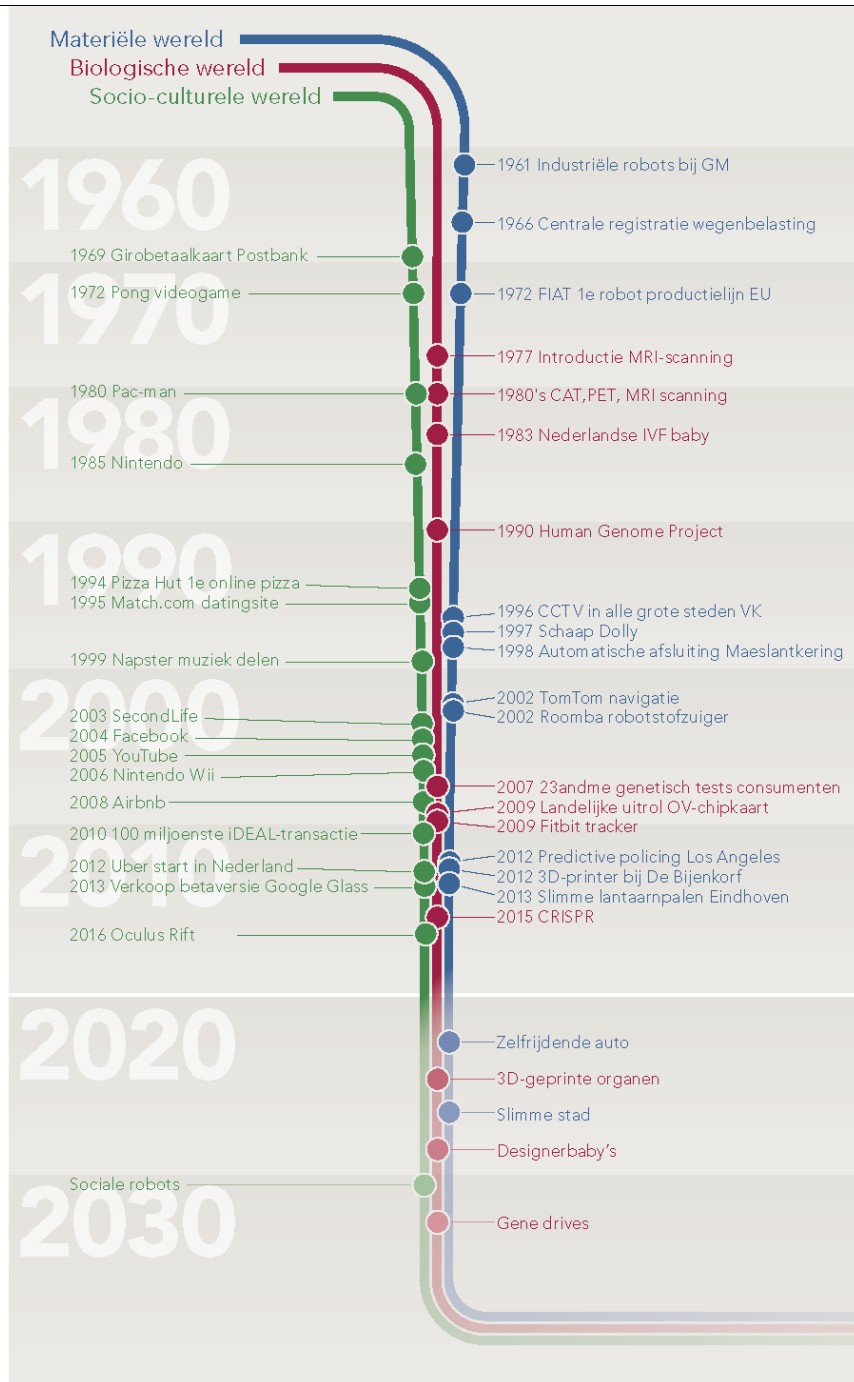
---

<sup>7</sup> [bbc.com/news/technology-35785875](http://bbc.com/news/technology-35785875),

<sup>8</sup> Een quantum computer maakt gebruik van de wetten van de quantumfysica en rekent met zogenaamde qubits. In tegenstelling tot de bits van een normale computer kunnen qubits op hetzelfde moment 0 en 1 zijn. Dat maakt het mogelijk om een berekening, die normaal gesproken uit elkaar opvolgende stappen bestaat, in één keer uit te voeren. Dat geeft een quantum computer radicale nieuwe mogelijkheden en een ongekeerde rekensnelheid.

De digitalisering van het materiële proces heeft niet alleen grote impact gehad op de muziekindustrie, maar ook onze culturele beleving van muziek beïnvloedt. Die invloed beschrijven we in de socio-culturele wereld. Ook het menselijk gedrag kent overlap tussen de biologische wereld en de socio-culturele wereld. Vanuit het bovengenoemde onderzoeksperspectief plaatsen we gedrag in de biologische wereld; we kijken naar gedrag als onderdeel van ons ‘mens zijn’ dat nu digitaliseert. Dat neemt niet weg dat gedrag naast biologische en psychologische factoren, sociale en culturele invloeden kent.

**Figuur 2.2** Overzicht mijlpalen van de digitalisering van de materiële, biologische en socio-culturele wereld





## Materiële wereld

De materiële wereld digitaliseert op allerlei manieren. Robots zien we niet meer alleen in de fabriek, maar komen we ook daarbuiten tegen. Camera's monitoren snelwegen, straten en stations. Apparaten in ons huis (slimme tv, slimme energiemeter) staan continu in verbinding met het internet en onze smartphone dragen we dag en nacht bij ons. In deze paragraaf illustreren we de digitalisering van de materiële wereld door te kijken naar 1) het productieproces, 2) de leefomgeving en openbare ruimte en 3) ons huis.

### *Productieproces*

Een belangrijke stap in de digitalisering van het productieproces is de intrede van mechanische robotarmen eind jaren zeventig in de maakindustrie. In de jaren tachtig en negentig drong ICT door als middel om het productieproces te optimaliseren en verspilling van bijvoorbeeld materiaalgebruik tegen te gaan.<sup>9</sup> De inzet van ICT ging hand in hand met de globalisering van de economie. Het werd steeds belangrijker om niet alleen het productieproces, maar ook de gehele keten te optimaliseren. Het verder opknippen van productietaken in deeltaken leidde tot zowel specialisering (outsourcing) als verplaatsing (offshoring). Ook maatwerk werd mogelijk. Klanten kunnen steeds vaker producten als sportschoenen zelf ontwerpen en online bestellen. De producten worden pas gemaakt na bestelling door de klant; ICT, in de vorm van flexibele computergestuurde productieprocessen, maakt *just-in-time* productie en massapersonalisatie (of *mass customisation*) mogelijk (zie Van Est & Kool 2015).

Sinds de jaren 2000 is het productie- en dienstenproces met nieuwe digitale middelen steeds nauwkeuriger te volgen. Er komt meer zicht op consumentengedrag en de manier waarop producten buiten de poort van de fabriek worden ingezet. De inzet van bijvoorbeeld RFID, GPS en videocamera's leidt bijvoorbeeld tot *high-resolution management* (Subirana et al. 2006, p. 11), of precisie-management. Dataverzameling en technieken voor monitoring en analyse staan daarin centraal. Er komt onder invloed van big data steeds meer informatie beschikbaar over alle onderdelen van de waardeketen, waardoor die nog efficiënter te organiseren is. Via continue monitoring van onderdelen van bijvoorbeeld auto's of treinen kunnen onderhoudskosten verlaagd worden. Zo ontstaat een slim wagenpark of treinenpark. De mogelijkheden tot dataverzameling, monitoring en analyse komen samen in toekomstbeelden die onder de noemer 'slim' of Internet of Things naar voren worden geschoven – een *Internet of Everything*: slimme energienetwerken, *smart mobility* (onder andere de zelfsturende auto), digitale oliewinning, robotmijnbouw, *smart farming* en slimme steden.

De inzet van een nieuwe generatie robots is een andere manier om het productieproces verder te optimaliseren. De capaciteiten van robots nemen toe, dankzij betere zichtsysteem (bijvoorbeeld door het gebruik van 3D-camera's), betere navigatiesystemen en vorderingen in de kunstmatige intelligentie. In de maakindustrie zijn robots niet meer weg te denken. De autonome fabriek is in Japan inmiddels werkelijkheid geworden, waar in de FANUC-fabriek robots een maand zonder toezicht kunnen werken (Royakkers & Van Est 2015). Ook buiten de fabriek laten robots zich meer zien. Voorbeelden daarvan zijn onbemande vliegtuigen (drones) en zelfsturende auto's,

---

<sup>9</sup> Het zogenoemde *lean management* principe, oorspronkelijk ontwikkeld in Japan.

dienstrobots in de zorg of de horeca, of huishoudelijke robots, zoals de robotstofzuiger. Wereldwijd ontstaan discussies over hoe robotica en kunstmatige intelligentie het werk van mensen in de toekomst zullen beïnvloeden (Ford 2015; Van Est & Kool 2015; Went et al. 2015; Brynjolfsson & McAfee 2014).

Digitale fabricatietechnologieën zoals 3D-printing vertroebelen de scheidslijn tussen digitale en materiële productieprocessen nog verder. Geavanceerde 3D-scanningstechnologieën maken het mogelijk om fysieke objecten om te zetten in eindeloos reproduceerbare digitale 3D-modellen. De schaal waarop materialen kunnen worden gecreëerd verschuift van micro, naar nano en atomair niveau: 'We're on the threshold of the third digital revolution, one in which matter and information merge,' stelt MIT-professor Gershenfield (Anthes 2006). In onderzoeksprojecten experimenteren wetenschappers met het printen van bloedvaten en organen. In 2013 werd een ontwerp voor een 3D-printbaar pistool online geplaatst.<sup>10</sup>

#### *Leefomgeving en openbare ruimte*

Ook de leefomgeving digitaliseert op allerlei manieren. Aan het eind van de jaren negentig introduceren gemeenten en bedrijven beveiligingscamera's in openbare ruimtes en bedrijventerreinen. In Nederland was Ede in 1997 de eerste gemeente die camera's plaatste. In de jaren daarna volgen camera's ons wegnnet, het openbaar vervoer en private ruimtes zoals winkels en bedrijven. Tegelijk met camera's doet ook andere digitale apparatuur zijn intrede in de openbare ruimte, zoals navigatie-apparaten, de ov-chipkaart en digitale stationspoortjes (Van 't Hof et al. 2010).

Door middel van smartphones, mobiel internet en sociale media raken de fysieke en virtuele wereld steeds nauwer met elkaar verweven. Sociale media, dating sites en andere diensten gaan locatie actief gebruiken als onderdeel van hun diensten (bijvoorbeeld bij *geo-tagging*, en 'inchecken' op locaties, of aan spellen gebaseerd op geografische elementen ('*geo-caching*'). Deze verwevenheid krijgt een nieuwe dimensie met de introductie van technieken als *virtual reality* en *augmented reality* (zie verder de socio-culturele wereld).

Onder de vlag van 'de slimme stad' digitaliseert onze leefomgeving de komende jaren nog verder: via allerlei sensoren kunnen overheden, bedrijven en bewoners gedetailleerd inzicht krijgen in processen in de stad. Telecombedrijven kunnen bijvoorbeeld op basis van de connecties die telefoons maken met hun zendmasten inzicht geven in hoe mensen zich door steden verplaatsen. Burgers kunnen met zelfgebouwde sensoren meten hoe verkeersstromen de plaatselijke luchtkwaliteit beïnvloeden. De slimme stad belooft een duurzame en comfortabele leefomgeving zonder files, energieverstopping of onzure steegjes. 'Slim' in deze context betekent dat ICT – software, sensoren en het internet – een digitale laag over de stad heen legt. Deze laag zorgt voor continue gegevensstromen, waarmee gemeenten gedrag van bewoners, verkeersdeelnemers of inbrekers kunnen monitoren of (bij)sturen. Een mogelijke toepassing kan bijvoorbeeld een slim riool zijn, dat bijhoudt welke bacteriën, biomarkers of virussen aanwezig zijn, zodat een mogelijke ziekte-

---

<sup>10</sup> 'The liberator' werd online beschikbaar gesteld door het bedrijf Defense Distributed en werd na 2 dagen offline gehaald door de Amerikaanse overheid (maar is wel op internet terug te vinden via p2p-sites).

uitbraak te voorspellen valt voordat mensen daadwerkelijk ziek worden,<sup>11</sup> of een slimme lantaarnpaal die zelf bepaalt wanneer hij aan gaat, met lichtkleuren de gemoedstoestand van voorbijgangers kan beïnvloeden en mogelijk agressie kan voorkomen, en met camera's voorbijkomend verkeer monitort.<sup>12</sup>

### *Huis*

Ook ons huis ontkomt niet aan de digitalisering. Via het Internet of Things krijgen allerlei huishoudelijke apparaten een internetadres. Ze worden 'aan het net' gehangen en krijgen sensoren, rekenkracht en communicatiemogelijkheden. Voorbeelden hiervan zijn slimme thermostaten die verbonden zijn met de energieleverancier en digitaal inzicht bieden in ons energieverbruik ten opzichte van anderen, of een slimme TV die ons kijkgedrag analyseert en ons op basis daarvan tips voor andere programma's geeft. Ook Barbie heeft inmiddels een microfoon en een internetverbinding.<sup>13</sup>

Het begrip Internet of Things stamt uit begin 2000, toen elektronicafabrikant LG een koelkast presenteerde die zijn inhoud zelf inventariseerde en automatisch contact zocht met de supermarkt om nieuwe voorraden te bestellen.<sup>14</sup> De term kreeg wereldwijd aandacht toen de Internationale Telecommunications Unit (ITU 2005) van de Verenigde Naties een rapport uitbracht over het onderwerp. Tien jaar later begon de visie van het Internet of Things werkelijkheid te worden. Verschillende markt bureaus verwachten de komende jaren een enorme groei van producten die verbonden zijn aan het internet. Gartner (2015) voorspelde in 2020 13,5 miljard verbonden objecten (op de consumentenmarkt), tegen 3 miljard in 2015. Ook de OESO schatte dat consumenten in Westerse landen in 2022 14 miljard *connected devices* in huis zullen hebben. Dat komt neer op ongeveer vijftig objecten per huishouden (OESO 2013).

### *Selectie technologiegebieden*

Uit deze paragraaf komen twee centrale technologieën naar voren die naar verwachting een belangrijke rol zullen spelen bij het vormgeven van de digitale samenleving de komende jaren: ontwikkelingen in de robotica en het Internet of Things / slimme omgevingen (zie tabel 2.1).

---

<sup>11</sup> Momenteel ontwikkeld door MIT Senseable City Lab, zie [underworlds.mit.edu](http://underworlds.mit.edu)

<sup>12</sup> Zoals in Eindhoven in het Living Lab Stratumseind 2.0' realiseert, zie [brainport.nl/high-tech-systems-materials/living-lab-laait-ander-licht-schijnen-op-stratumseind](http://brainport.nl/high-tech-systems-materials/living-lab-laait-ander-licht-schijnen-op-stratumseind)

<sup>13</sup> De pop neemt gesprekken op, en stuurt die naar de cloud. Kunstmatige intelligentie helpt bij de analyse van het gesprek, en kiest op basis daarvan een passend antwoord. Eind 2015 kwam Barbie negatief in het nieuws doordat het mogelijk bleek de opgenomen gesprekken te hacken.

<sup>14</sup> Het concept dat LG in 2000 presenteerde werd in 2016 werkelijkheid. Op de CES-beurs presenteerde Samsung de slimme koelkast voor de consumentenmarkt die in de loop van 2016 daadwerkelijk te koop zal zijn (inclusief bijbehorende diensten) in Zuid-Korea.

**Tabel 2.1** Selectie technologiegebieden materiële wereld

Technologiegebied	Omschrijving
Robotica	Robots kunnen steeds complexere taken uitvoeren. Ze krijgen beter zicht (3D-beeld), kunnen beter navigeren en zich bewegen, en slimmer interacteren met mensen. Robots zijn nu te vinden in fabriekshallen, maar de verwachting is dat sociale robots een rol zullen gaan spelen in kantoren, schoolgebouwen, ziekenhuizen, restaurants en de thuisomgeving.
Internet of Things en slimme omgevingen	Objecten worden in toenemende mate uitgerust met een internetverbinding, sensoren, rekenkracht en communicatiemogelijkheden. Zo verzamelt het object gegevens over zijn omgeving, die het kan delen met andere objecten ( <i>machine 2 machine</i> communicatie) om processen aan te sturen, of in de <i>cloud</i> analyseert om informatie of diensten 'op maat' aan te bieden.

## Biologische wereld

In de afgelopen zes decennia digitaliseerde ook de biologische wereld. Gedrag, emoties, lichaamsfuncties en het menselijk DNA waren steeds beter te vangen in bits en bytes en door software te analyseren. Het genetisch materiaal van de mens is in de afgelopen jaren digitaal in kaart gebracht, en kan ook bewust worden aangepast. Via *smart wearables* verzamelden gebruikers en bedrijven biologische gegevens zoals hartslag, ademhalingsfrequentie, lichaamstemperatuur en voedings- en slaappatronen. En in de toekomst bieden onze oorschelp, looppatroon, stemgeluid, houding, ademhaling, hartslag en zelfs de manier waarop we typen nieuwe manieren om mensen te identificeren. In deze paragraaf illustreren we de digitalisering van de biologische wereld door te kijken naar 1) het menselijk lichaam 2) het brein en 3) het menselijk gedrag.

### *Lichaam*

De digitalisering van het lichaam begon decennia geleden met de inzet van medische apparatuur die het lichaam 'digitaal' kunnen uitlezen. Aanvankelijk gebeurde dat via technieken als röntgenbeelden en CT-scans, of bloedglucosemeters voor diabetici. Een belangrijke ontwikkeling voor de digitalisering van de 'code' van het lichaam was het Human Genome Project. Het project startte in 1990 en bracht de structuur van het menselijk DNA in kaart. Bij aanvang schatte men dat dit circa vijftien jaar zou duren, maar door de enorme vooruitgang in de gebruikte DNA-analysetechnieken – mede mogelijk gemaakt door de snelle ontwikkeling in computerrekenkracht en opslagcapaciteit – was al in 2000 een eerste ruwe kaart gereed. In de jaren daarna werd het mogelijk om DNA-materiaal ook aan te passen. Recent is dit door de CRISPR-editing techniek goedkoper, sneller en gemakkelijker geworden (zie kader 2.2). De techniek brengt omstreden toekomstbeelden over designerbaby's een stap dichterbij.

### Kader 2.2 CRISPR

In de afgelopen jaren is het uitlezen van het menselijk genoom steeds makkelijker geworden met ontwikkelingen in *genome-sequencing*-technologie. Het aanpassen van genetische informatie was echter tot voor kort nog een moeilijke opgave. De ontwikkeling van de CRISPR-Cas9-technologie (vaak kortweg CRISPR genoemd) heeft daarin voor veel opschudding gezorgd. De CRISPR-technologie maakt gebruik van het natuurlijke afweersysteem van bacteriën. Wanneer bacteriën worden geïnficeerd met een virus bouwen ze een deel van dat virus in hun eigen DNA in om het in de toekomst te kunnen herkennen. Wetenschappers pasten het systeem zo aan dat ze kunnen selecteren welk stukje DNA wordt ingebouwd en waar dat in het DNA gebeurt. Bovendien kan de techniek naast bacteriën ook op dieren en mensen worden toegepast. Op deze manier maakt CRISPR het makkelijker, sneller en goedkoper om de genen van bacteriën, planten, dieren en mensen aan te passen.

Ook buiten het laboratorium is de digitalisering van het lichaam zichtbaar. In de gezondheidszorg wordt gebruikgemaakt van de techniek om snel en goedkoop DNA af te lezen (Next Generation Sequencing). De techniek helpt klinisch-genetische centra bij het vinden van een oorzaak bij een ziektebeeld. Er zijn hoge verwachtingen over het bieden van gezondheid op maat door meer kennis over iemands DNA-profiel, maar voorlopig is dit nog toekomstmuziek (Vrijenhoek & Radstake 2016). Sinds 2006 kunnen mensen via commerciële diensten als 23andMe inzicht krijgen in hun eigen genetisch profiel en in mogelijke erfelijke aanleg voor aandoeningen en eigenschappen zoals kaalheid of blindheid. Naast genetische informatie zien de we digitalisering van het lichaam ook op allerlei andere vlakken. De huidige generatie smartphones en apps bieden hulp aan mensen om zelf hun bloeddruk, glucose, hartslagvariabiliteit en stressreacties te monitoren. Van toekomstige generatie digitale coachingsapparaten wordt verwacht dat ze met behulp van kleinere en betere sensoren de psychofysiologische staat van gebruikers voortdurend kunnen monitoren (Kool et al. 2014).

### Breïn

Ook (delen) van ons brein digitaliseren. Zo helpt *neuro-imaging*-technologie in het lab om cognitieve processen in kaart te brengen. Wetenschappers werken met behulp van *deep brain stimulation* (DBS) aan breinimplantaten om bijvoorbeeld de trillingen van Parkinsonpatiënten te verminderen. Een geïmplanteerde neurostimulator, stuurt elektrische pulsen naar een elektrode die operatief is aangebracht in de hersenen, al naargelang de stoornis op een specifieke plek. In 2011 hadden hier al meer dan 70.000 parkinsonpatiënten gebruik van gemaakt (Bronstein et al. 2012). Wetenschappers werken ook aan andere toepassingen van DBS, bijvoorbeeld om depressie te verhelpen. In het consumentendomein komen *brain-computer interfaces* op de markt waarmee gebruikers zelf hun hersengolven kunnen analyseren en hun cognitieve vermogens proberen te verbeteren. *Do-it-yourself* neuro-enhancers proberen met elektrische golven hun eigen breincapaciteit te vergroten of trainen hun concentratie met feedback over patronen in hun hersengolven (Burkeman 2014).

Emotieherkenningstechnologie leert onze emoties steeds beter herkennen. De software voor dat doel is de laatste jaren zoveel vooruit gegaan dat computers gemiddeld beter zijn dan mensen in het herkennen van een valse emotie (Andrade 2014; Li et al. 2015). Ook gezichtsherkenningstechnologie verbetert snel. De beste algoritmen herkennen gezichten inmiddels net zo goed als mensen dat doen (Harris 2015). Gezichts- en emotieherkenning zijn onderdeel van een reeks nieuwe identificatiemogelijkheden op basis van het menselijk lichaam, naast bekende methoden als de vingerafdruk en de irisscan (Janssen et al. 2014).

### *Gedrag*

De laatste jaren ontdekken wetenschappers en bedrijven dat er ook allerlei informatie uit ons digitale surfgedrag valt af te leiden. Dit komt door de combinatie van de aanwezigheid van grote hoeveelheden digitale, persoonlijke gegevens én slimme software om die gegevens te analyseren. Facebookprofielen geven bijvoorbeeld informatie over seksuele geaardheid of politieke voorkeuren (Kosinski et al. 2013). Watson van IBM heeft genoeg aan een A4'tje tekst om een persoonlijkheidsanalyse van de auteur te maken. En het recruitment bedrijf Entelo scout talentvolle programmeurs op basis van wat ze op het internet posten (Peck 2013). In de digitale wereld gaan we nader in op de inzet van big data en slimme software.

Na het herkennen en het analyseren van menselijk gedrag, is het beïnvloeden van gedrag een volgende stap (zie kader 2.3). Denk aan Facebook's emotiestudie, waarbij bleek dat het tonen van positieve of negatieve informatie de stemming van gebruikers beïnvloedt. Gebruikers gaan hierdoor zelf ook meer positieve of negatieve posts plaatsen. De studie leidde tot grote ophef onder gebruikers toen bekend werd dat zij ongemerkt onderdeel waren van een experiment (Adam et al. 2014). Ook het ongemerkt personaliseren van zoekgedrag door zoekmachines als Google is een voorbeeld van subtiele beïnvloeding (Van 't Hof et al. 2012).

### **Kader 2.3 Persuasieve technologie**

Persuasieve technologie maakt gebruik van inzichten uit de psychologie, gedragswetenschappen en mens-computerinteractie, om systemen te ontwerpen die gebruikers aanzetten tot gedragsverandering (Fogg 2002). Dit soort technologische gedragsbeïnvloeding – ook wel *nudging* genoemd – wordt steeds geraffineerder. Zo wordt er gekeken naar gepersonaliseerde beïnvloedingsstrategieën, waarbij gebruikers worden beïnvloed met het soort argumentatie waar zij gevoelig voor zijn (Kaptein 2015; Kaptein & Eckles 2012). Met *ambient feedback* kijken onderzoekers hoe mensen op een laag cognitief bewust niveau zijn te beïnvloeden met elementen uit hun omgeving, zoals licht of kleur. Onderzoek naar laagcognitieve beïnvloeding met kleur laat zien dat dit een effectieve strategie kan zijn. Systemen die feedback geven met behulp van kleur over het energieverbruik lijken effectiever dan op cijfers gebaseerde feedback (Maan et al. 2011; Ham et al. 2009).

### *Selectie technologiegebieden*

Uit deze paragraaf komen verschillende technologieën naar voren die naar verwachting de komende jaren de digitale samenleving verder zullen vormgeven. Een aantal daarvan wordt uitvoerig besproken in het medisch ethische, en bio-ethische domein, waaronder CRISPR en *deep*

*brain stimulation* (zie bijvoorbeeld Van Est et al. 2014; Van Est et al. 2016). We richten ons hier daarom vooral op de gebieden die zich buiten het medische domein bevinden. Dat zijn 1) de snelle verbeteringen op het gebied van gezichtsherkenning en andere lichaamskenmerken (multimodale biometrie), en 2) de groeiende inzet van persuasieve technologie in het consumentendomein (zie tabel 2.2). Andere in deze paragraaf besproken technologieën hebben betrekking op het analyseren van menselijk gedrag via *data analytics*. Deze technieken bespreken we bij de digitale wereld (paragraaf 2.4).

**Tabel 2.2** Selectie technologiegebieden biologische wereld

Technologiegebied	Omschrijving
Persuasieve technologie	Persuasieve technologie heeft als doel om het menselijk gedrag te beïnvloeden en te veranderen. De methoden voor beïnvloeding worden steeds subtieler.
Multimodale biometrie	Biometrie is een manier om mensen uniek te identificeren, met behulp van verschillende <i>identifiers</i> van het menselijk lichaam: vingerafdruk, iris, stemgeluid, gezicht, oorschelpen, hartritme of looppatroon. De toekomstverwachting is dat door het combineren van deze verschillende modaliteiten, het identificeren van mensen makkelijker wordt. De technologie kent ook andere toepassingen, bijvoorbeeld als beveiliging.

Rathenau Instituut

## Socio-culturele wereld

Het groeiende gebruik van ICT betekent ook digitalisering van interacties tussen mensen; tussen mensen onderling en tussen mensen en organisaties. Digitalisering dringt door in ons sociale en culturele leven: shoppen, muziek luisteren, contact met vrienden, actie voeren, het vinden van dates doen we in toenemende mate online. Zelfs na de dood kunnen onze digitale profielen op diensten als LivesOn<sup>15</sup> nog voor ons blijven praten. Het onderscheid tussen offline en online is steeds moeilijker te maken. Ook organisaties digitaliseren: steeds meer klantcontact verloopt geheel digitaal en er ontstaan nieuwe, digitale disruptieve organisatiemodellen waarbij het organiseren en toegang geven tot producten en diensten belangrijker is dan het zelf maken of eigenaar zijn van die producten of diensten. Het inmiddels beroemde citaat van Tom Goodwin, vice-president van Havas Media, laat het succes van deze nieuwe organisatiemodellen zien: ‘Uber, the world’s largest taxi company, owns no vehicles. Facebook, the world’s most popular media owner, creates no content. Alibaba, the most valuable retailer, has no inventory. And Airbnb, the world’s largest accommodation provider, owns no real estate. Something interesting is happening.’ Goodwin (2015). In deze paragraaf illustreren we de digitalisering van de socio-culturele wereld door te kijken naar 1) de digitalisering van communicatie en cultuur en 2) digitalisering van organisatiemodellen.

<sup>15</sup> [liveson.org/connect.php](http://liveson.org/connect.php)

### *Communicatie en cultuur*

De komst van sociale media en andere online diensten eind de jaren negentig en na de eeuwwisseling hebben grote impact op onze manier van communiceren. De diensten verwerven een steeds belangrijker rol in onze cultuur en bij het vormgeven van onze identiteit. Zie bijvoorbeeld Boyd (2014) over het leven van de genetwerkte jeugd, het werk van Turkle over de impact van het scherm op ons leven en relaties (Turkle 2015; 2011) of van Carr over mogelijke andere (meer oppervlakkige) werking van ons brein door het internet (2010). We vergroeien met onze smartphone, die dé verbinding vormt tussen het fysieke en virtuele leven. Floridi et al. (2014) kenmerken dit als onlife: het onderscheid tussen offline en online leven is niet meer te maken; ze zijn één geworden.

Recente ontwikkelingen in *virtual reality* en *augmented reality* dragen ook bij aan deze versmelting. Via *virtual reality* (VR) kunnen gebruikers virtuele ervaringen 'echter' of beter voelen. Gamemakers passen de techniek toe om gamers meer op te laten gaan in hun spel. Ook andere domeinen maken gebruik van VR, zoals de zorg voor het revalideren van een lichamelijke handicap of in het leger om militairen te trainen. Via *augmented reality* (AR) kunnen gebruikers real-time extra informatie krijgen. Denk bijvoorbeeld aan de app Layar die huizenzoekers ter plekke informatie geeft over een bepaald huis dat zij in de omgeving zien. Ook in de professionele omgeving biedt de techniek mogelijkheden. Een monteur kan bijvoorbeeld terwijl hij aan het werk is via zijn slimme bril opzoeken hoe een bepaalde handeling ook alweer moest en een chirurg kan continu informatie krijgen over vitale functies van zijn patiënt.

Ook culturele producten en diensten digitaliseren: muziek, boeken, films en spellen zijn geheel digitaal te maken, te distribueren, te beluisteren, te lezen, te bekijken en te spelen. Slimme aanbevelingstechnologie, gebruikmakend van big data en inzichten uit de kunstmatige intelligentie, helpt mensen bij het maken van een keuze uit het enorme aanbod. De snelle ontwikkeling van kunstmatige intelligentie zorgt ervoor dat software ook dingen kan die we tot voor kort als exclusief 'menselijk' beschouwden. Zo kan software (in beperkte mate) journalistieke bijdragen schrijven in domeinen als sport of de financiële beurzen. Watson, de slimme computer van IBM, wint taalspelletjes als Jeopardy! en als chef won hij in 2015 de Horecava Innovation Award. Software componeert ook symfonieën die experts niet van menselijke topcomponisten kunnen onderscheiden (Steiner 2012).

### *Organisatiemodellen*

De interactie tussen organisaties en consumenten verloopt eveneens steeds meer geheel digitaal. Daardoor veranderen ook organisatiemodellen. Er zijn steeds meer webwinkels zonder fysieke winkel en organisaties proberen steeds vaker contact te leggen met hun klanten via digitale kanalen (Twitter, chat, mail, apps). Ook de overheid hanteert sinds een paar jaar als uitgangspunt 'digitaal als het kan, persoonlijk als het moet' (BZK 2013).

Vanaf de eeuwwisseling ontstonden er digitale organisatiemodellen die een centrale rol speelden in het organiseren en faciliteren van transacties in de economie en maatschappij (Kreijveld et al. 2014). Zo ging er een innovatieve impuls uit van appstores doordat softwareontwikkeling via dit platform toegankelijk werd voor kleine onafhankelijke spelers. Onderdeel van het succes is het innemen van een strategische positie tussen verkoper en koper, zoals Apple zich met iTunes



tussen de artiesten, platenmaatschappijen en consument heeft geplaatst (Kreijveld et al. 2014). Vanaf 2010 ontstaan er radicale nieuwe organisatievormen door deze digitale platformen. Voorbeelden zijn Airbnb en Uber die in enkele jaren zijn uitgegroeid tot grote economische spelers, die hun respectievelijke branches drastisch verstoren. Ismail et al. (2014) spreken van exponentiële organisaties die zo min mogelijk vaste medewerkers en zo veel mogelijk personeel op afroep willen hebben, optimaal gebruikmaken van de gratis diensten van een digitale gemeenschap, maximaal gebruikmaken van geautomatiseerde algoritmen en zo min mogelijk kapitaalgoederen in eigen bezit hebben. Een ander voorbeeld van een digitaal platform is de blockchaintechnologie. Deze technologie maakt het mogelijk om zogenaamde autonome organisaties te ontwikkelen: organisaties die volledig uit bits en bytes bestaan. De technologie kan een set van afspraken en taken automatiseren en zo de functie van een bepaalde organisatie overnemen (zie kader 2.4).

#### **Kader 2.4 Blockchain**

De *blockchain* is bekend als het achterliggende technisch protocol waarop de virtuele munt *Bitcoin* is gebaseerd. Simpel gezegd werkt de blockchain als een virtueel kasboek, dat alle transacties tussen gebruikers vastlegt. Het kasboek wordt op alle computers die deel uitmaken van het blockchainnetwerk bijgehouden en is met slimme cryptografie versleuteld. Elke nieuwe transactie wordt door heel het netwerk verspreid en gecontroleerd. Het principe achter het blockchainprotocol kan allerlei soorten afspraken vastleggen. Daardoor wordt het mogelijk om contracten of zelfs volledige organisaties – *Distributed Autonomous Organisations* (DAOs) – te automatiseren. Een voorbeeld is een webhostingbedrijf dat websitedomeinen verkoopt: in de software wordt vastgelegd dat als voor een bepaald moment, een bepaalde partij, een bepaald bedrag betaalt op een bepaalde rekening, dat het eigenaarschap van domeinnaam X dan overgaat naar die partij. Of een verzekering: de blockchain zou de afspraak kunnen automatiseren dat mensen een bepaald bedrag in een pot storten en in geval van een ongeval een schadevergoeding krijgen.

#### *Selectie technologiegebieden*

Uit deze paragraaf behandelen we twee centrale technologiegebieden die naar verwachting de komende jaren de digitale samenleving vormgeven: 1) de verdere ontwikkeling van sociale media, onder andere via technieken als virtual reality en augmented reality, en 2) digitale platformen inclusief blockchaintechnologie (zie tabel 2.3).

**Tabel 2.3** Selectie technologiegebieden socio-culturele wereld

Technologiegebied	Omschrijving
Sociale media (incl. VR en AR)	Via sociale media en onze smartphone versmelten het virtuele en fysieke leven. Een volgende stap voor deze versmelting is het toepassen van virtual reality en augmented reality
Digitale platformen (incl. blockchain)	Digitale organisatiemodellen vormen een steeds belangrijkere rol in het organiseren en faciliteren van transacties in de economie en maatschappij. Overal ontstaan nieuwe digitale platformen die verstorend werken voor 'oude' organisatiemodellen.

Rathenau Instituut

## 2.4 De digitale wereld

De vorige paragraaf beschreef hoe vele aspecten uit de materiële, biologische en socio-culturele wereld inmiddels een digitale representatie hebben gekregen. Dat leidde tot een almaar groeiende digitale wereld. In deze paragraaf illustreren we de digitale wereld door te kijken naar 1) big data en algoritmen en 2) kunstmatige intelligentie.

### *Big data en algoritmen*

In 2011 berekende consultancybedrijf IDC dat het digitale omniversum bestond uit 1,8 'zettabytes'. Omgerekend in Apple iPad's komt dat neer op genoeg tablets om een Chinese muur van te bouwen, twee keer zo hoog als het origineel (IDC 2011). Sindsdien is de omvang van de digitale wereld exponentieel gegroeid en lijkt zijn eigen 'wet van Moore' te kennen: elke twee tot drie jaar verdubbelt de hoeveelheid data (Mayer-Schonberger & Cukier 2013b; IDC 2014); een fenomeen dat inmiddels bekend staat als 'big data'.<sup>16</sup> De data zijn bijvoorbeeld afkomstig van camera's, smartphones, tablets en andere draagbare apparaten, of van browsers en sociale netwerken. Elke dag uploaden gebruikers bijvoorbeeld meer dan tien miljoen nieuwe foto's naar Facebook. Andere databronnen zijn clouddiensten, en de toenemende toepassing van sensoren in producten en machines, die non-stop in verbinding staan met het internet.

Die almaar uitdijende digitale wereld betekent ook dat we steeds afhankelijker zijn van slimme algoritmen (software) om informatie te halen uit alle bits en bytes. Dataverzamelingen en data-analyses worden steeds complexer van aard. Bedrijven en overheden zetten (zelflerende) software vaker in om processen efficiënter te laten verlopen, bijvoorbeeld op de beurs, bij het verstrekken van krediet, bij het opsporen van fraude, of bij het reguleren van content op sociale media.<sup>17</sup> Dat gaat niet altijd goed, en het kan lastig zijn om te achterhalen op basis van welke informatie software

<sup>16</sup> Er is geen eenduidige definitie van big data. Sommigen verwijzen naar de kenmerken van big data: volume, variety en velocity (de 3 V's) (Gartner 2011). Voora anderen gaat het naast hoeveelheid ook om de combinatie van die datahoeveelheden en software die bijvoorbeeld op basis van patroonherkenning en correlaties onverwachte – waardevolle – verbanden kan vinden.

<sup>17</sup> Bij het reguleren van content op websites en fora bepaalt software automatisch wat wel en niet door de beugel kan (zoals discriminerende teksten of hatelijke uitlatingen). De Russische internetcriticus Yevgeni Morozov stelde in 2014 dat de software van Silicon Valley daarmee de samenleving een nieuw soort conservativiteit oplegt, waarbij algoritmes bepalen wat cultureel wel of niet is toegestaan (Morozov 2014).

tot een bepaald inzicht is gekomen. Naarmate software vaker automatisch beslissingen neemt, neemt het belang van controle op die systemen toe. Ook hier kan technologie een rol spelen. Met WatsonPaths probeert IBM bijvoorbeeld een medisch beslissingsstelsel te creëren dat uitleg kan geven over welke informatie en bronnen het stelsel geraadpleegd heeft, en welke paden het heeft verkend bij het komen tot een antwoord (IBM 2013).

### *Kunstmatige intelligentie*

Dataminingstechnieken (*data analytics*) en kunstmatige intelligentie (met name technieken als *deep learning*) profiteren enorm van de grote hoeveelheden gegevens die de afgelopen jaren beschikbaar zijn gekomen (zie kader 2.5). De data vormen trainingsbestanden voor zelflerende software: hoe meer data de software krijgt, hoe slimmer die wordt. De gezichtsherkenningsoftware van bedrijven als Facebook en Google verbetert zo snel dankzij de vele foto's die gebruikers elke dag uploaden. Ook vertaalsoftware verbetert doordat het kan putten uit een groot aantal officiële vertaalde documenten, van de Verenigde Naties en de Europese Commissie (Mayer-Schonberger & Cukier 2013).

#### **Kader 2.5 Deep learning**

*Deep learning* is een vorm van machineren die zwaar leunt op statistisch rekenwerk en neurale netwerken en mede mogelijk wordt door de opkomst van big data (The Economist 2015). In plaats van te proberen de regels te definiëren die een computer moet gebruiken om bijvoorbeeld taal te 'begrijpen', maken computerwetenschappers gebruik van de toenemende hoeveelheden data om software verbanden of regels te laten ontdekken. Via *deep learning* abstraheren computers informatie op basis van verschillende lagen van neurale netwerken. Bij beeldverwerking krijgt de eerste laag bijvoorbeeld ruwe beelden te zien, die contrast en kleuren probeert te identificeren. Een tweede laag combineert die informatie en zoekt naar meer abstracte observaties, zoals randen of schaduwen. De volgende laag kijkt of het daarmee ogen, lippen of oren kan identificeren, waardoor het willekeurige gezichten kan herkennen (The Economist 2015). Nu leren deze modellen nog met behulp van mensen, die aangeven of een beeld een gezicht is of niet, maar er wordt ook gewerkt aan *unsupervised learning* waarbij de software leert op basis van zelfexploratie en zelfcorrectie.

### *Selectie technologiegebieden*

Uit deze paragraaf komen twee centrale technologiegebieden naar voren die naar verwachting de komende jaren de digitale samenleving vormgeven: 1) big data en algoritmen en 2) kunstmatige intelligentie. Veel van de technologiegebieden die werden behandeld in de voorafgaande paragrafen leunen (deels) op de vooruitgang in kunstmatige intelligentie en big data (tabel 2.4).

**Tabel 2.4** Selectie technologiegebieden digitale wereld

Technologiegebied	Omschrijving
Big data en algoritmen	Om informatie (verbanden en patronen) te halen uit de groeiende digitale wereld, zijn algoritmen steeds belangrijker.
Kunstmatige intelligentie ( <i>deep learning</i> )	Kunstmatige intelligentie – het geven van een vorm van intelligentie aan een systeem – ondersteunt allerlei technologische toepassingen (bijvoorbeeld in de robotica, taalverwerking of slimme omgevingen), en vindt haar weg in steeds meer softwaretoepassingen.

Rathenau Instituut

## 2.5 De vier werelden bijeen: een nieuwe fase in de digitale samenleving

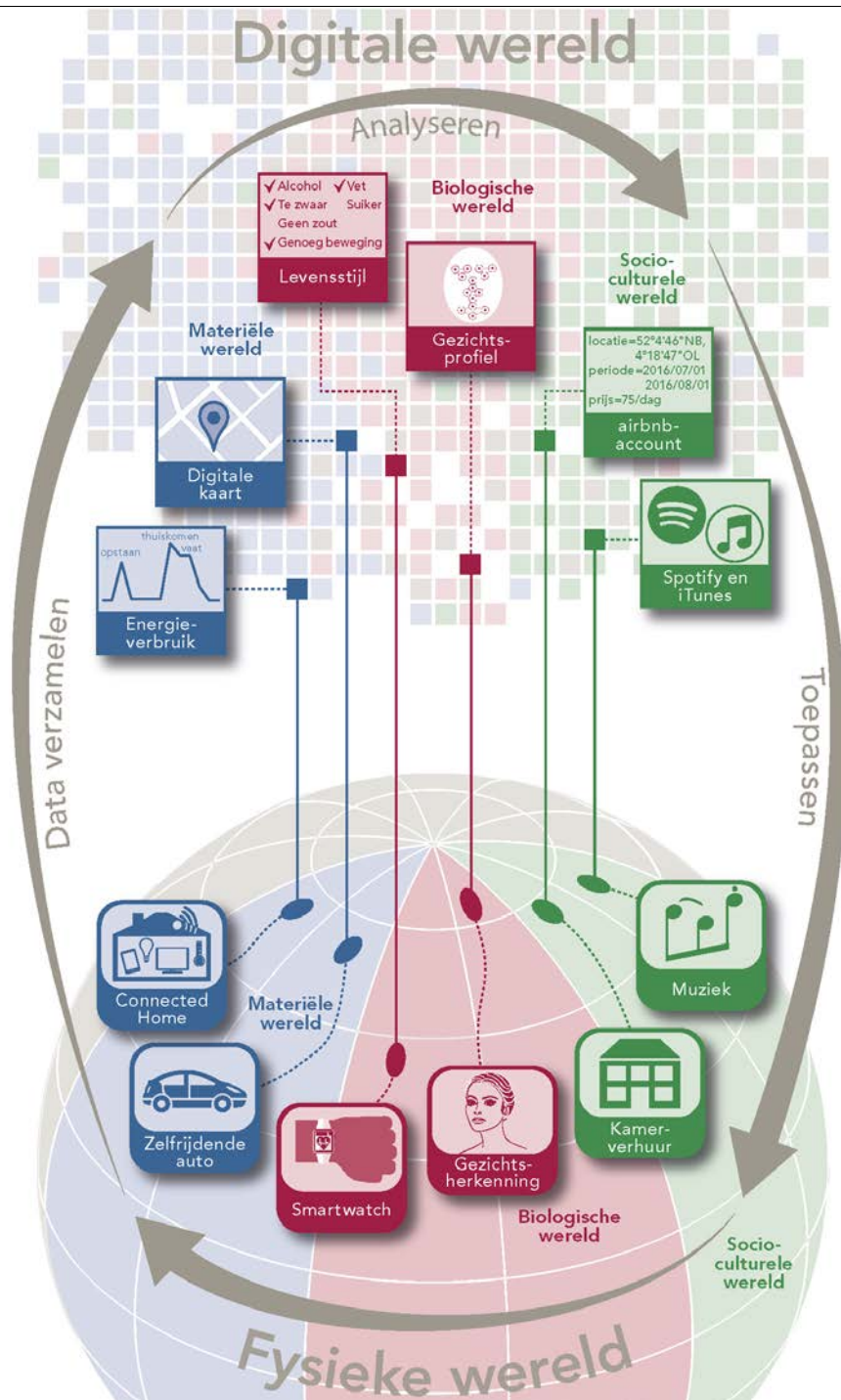
In het voorgaande hebben we de *objecten* van digitalisering besproken. De materiële wereld, de biologische en de sociale wereld zijn de afgelopen jaren steeds verder gedigitaliseerd, met een almaar uitdijende digitale wereld tot gevolg. Waar digitalisering aanvankelijk begon met het verzamelen van gegevens over (delen van) de materiële, biologische en sociale wereld, is het nu mogelijk om deze gegevens op grote schaal te analyseren en de opgedane kennis direct weer toe te passen in de fysieke wereld. Een treinfabrikant kan bijvoorbeeld via sensoren zijn treinenpark monitoren, preventief onderhoud plegen en tegelijkertijd zijn technici aanstuurt. Of de zelfsturende auto die gebruik maakt van digitale kaarten en met elke meter die hij rijdt ook informatie toevoegt aan die digitale kaart, en zo de kaart verbetert. Of datasurveillance, waarin bedrijven acties van gebruikers volgen, profileren en op basis daarvan real-time ‘passende’ informatie, producten of prijzen tonen (zie figuur 2.3).

Er ontstaan door de verknoping van de vier werelden continue *feedback-loops* tussen de fysieke en digitale wereld die op allerlei terreinen zichtbaar zijn: het productieproces, de omgeving, het lichaam, en ons gedrag. Hoewel digitalisering al decennialang aan de gang is, is het recent steeds makkelijker geworden om op steeds gedetailleerder niveau, real-time in te interveniëren in de fysieke wereld. Daarmee lijken ze een nieuwe fase in de ontwikkeling van de digitale samenleving in te luiden; een fase waarin een *cybernetische loop* ontstaat tussen de fysieke en de digitale wereld (zie figuur 2.3). Dat betekent dat processen in de fysieke wereld worden gemeten, die hieruit voortkomende data wordt geanalyseerd, en er vervolgens real-time op gedetailleerd niveau wordt ingegrepen. Het effect van de interventie kan vervolgens weer worden gemeten, geanalyseerd en worden bijgesteld om weer een volgende cyclus van de cybernetische loop te doorlopen.

We zien daarmee een terugkeer van het zogenaamde ‘cybernetische denken’ dat in de jaren ‘50 en ‘60 in de belangstelling stond. De basisgedachte van de cybernetica is dat biologische, sociale en cognitieve processen begrepen kunnen worden in termen van informatieprocessen en -systemen, en dus ook digitaal zijn te programmeren en aan te sturen (de Mul 1999). Inmiddels staat sturing met ICT weer volop in de schijnwerpers. Overal ontstaan toekomstvisies over slimme omgevingen

gericht op digitale sturing: slimme steden, slimme energienetwerken, slimme fabrieken, ziekenhuizen, kantoren, huizen enzovoorts. Digitale sturing biedt de samenleving en de individuen in die samenleving allerlei kansen: van goedkoper of duurzamer produceren, tot het vroegtijdig opsporen of voorkomen van ziektes. Maar het leidt ook tot zorgen, bijvoorbeeld over het manipuleren van menselijk gedrag en over wat ons mens maakt. In het volgende hoofdstuk gaan we dieper op deze ethische en maatschappelijke kwesties in.

**Figuur 2.3** Cybernetische feedback-loop tussen de digitale en fysieke wereld



## 2.6 Tot slot

De centrale vraag in dit hoofdstuk was hoe we de digitalisering van de samenleving kunnen begrijpen. We brachten de middelen om te digitaliseren in kaart, zoals computers, software en het internet, en lieten zien hoe nieuwe objecten uit onze omgeving digitaliseren. Steeds meer delen uit de materiële wereld, de biologische wereld en de socio-culturele wereld krijgen een virtuele representatie in de digitale wereld. Tot slot blijkt dat digitalisering geen nieuwe ontwikkeling is, maar dat – nu er zoveel zaken uit ons leven gedigitaliseerd zijn – er een nieuwe fase in de digitale samenleving lijkt aangebroken: een continue feedback-loop en interactie tussen de fysieke en virtuele wereld, die real-time interveniëren mogelijk maakt.

We selecteerden acht technologiegebieden die naar verwachting de komende jaren de digitale samenleving zullen vormgeven (zie tabel 2.5). In het volgende hoofdstuk gebruiken we deze technologiegebieden om de maatschappelijk en ethische kwesties zij oproepen te analyseren.

**Tabel 2.5** Selectie technologiegebieden

Materiële wereld	Biologische wereld	Socio-culturele wereld	Digitale wereld
Robotica	Persuasieve technologie	Platformen	Kunstmatige intelligentie
Internet of Things	Multimodale biometrie	VR/AR en sociale media	Big data en algoritmen

# 3 Maatschappelijke en ethische issues van digitalisering

## 3.1 Inleiding

De digitalisering van de samenleving verlegt de grenzen van ons kunnen en biedt allerlei mogelijkheden, maar daagt ook onze morele grenzen uit. In dit hoofdstuk beschrijven we welke maatschappelijke en ethische vragen er door de digitalisering van de samenleving worden opgeroepen.<sup>18</sup> Dat doen we aan de hand van voorbeelden uit de in het vorige hoofdstuk geselecteerde technologiegebieden: Internet of Things, robotica, biometrie, persuasieve technologie, virtual & augmented reality, digitale platformen, big data, slimme algoritmen en kunstmatige intelligentie. Onze beschrijving is daarmee niet uitputtend maar geeft een beeld van de verschillende soorten maatschappelijke en ethische issues die opkomen als gevolg van digitalisering. We benaderen ethiek als de systematische reflectie op moraal, het geheel van normen en waarden die feitelijk bestaan in een samenleving (zie kader 3.1). We zien ethiek dus niet als iets dat alleen op individueel niveau speelt, maar kijken vanuit de ethische waarden in een samenleving (zowel individueel als maatschappelijk).

### Kader 3.1: Ethische en maatschappelijke vragen

In dit hoofdstuk gaan we in op de maatschappelijke en ethische kwesties die door de digitalisering worden opgeroepen. Wat ethiek precies is, is geen makkelijke kwestie. Ethiek definiëren we hier als de systematische reflectie op moraal, het geheel van normen en waarden die feitelijk bestaan in een samenleving. Een dergelijke reflectie kan de vaardigheid vergroten om met morele problemen die samenhangen met de digitalisering om te gaan. Door de ontwikkelingen binnen de geselecteerde technologiegebieden zal onze samenleving steeds verder digitaliseren. Dit roept de vraag op hoe we deze digitale samenleving op een maatschappelijk en ethisch verantwoorde manier vorm kunnen geven. We zullen aan de hand van de geselecteerde technologiegebieden laten zien dat er bij het digitaliseren van de samenleving veel ontwikkelingen zijn die op gespannen voet lijken te staan met ethische waarden, zoals privacy en autonomie. Dit hoofdstuk brengt die ethische waarden in kaart. De vervolgvraag is dan hoe we deze ethische waarden kunnen waarborgen oftewel hoe we diverse relevante waarden zo goed mogelijk kunnen beschermen. Die governancevraag staat centraal in het volgende hoofdstuk.

---

<sup>18</sup> We erkennen de vele positieve impacts die de ontwikkeling van digitalisering heeft. Omdat het doel van deze tekst is om zicht te krijgen op de plekken waar ethische en maatschappelijke waarden in het geding zijn zullen hier vooral de situaties worden besproken waar digitalisering mogelijk onwenselijke impacts heeft.

In lijn met het vorige hoofdstuk structureren dit hoofdstuk door te kijken naar welke vraagstukken in de materiële (paragraaf 3.2), biologische (paragraaf 3.3), socio-culturele (paragraaf 3.4) en de digitale wereld (paragraaf 3.5) naar voren komen. Het overzicht is niet uitputtend, maar geeft een beeld van de meest prominente vraagstukken en de ontwikkeling die hierin plaatsvindt. In onze analyse van de wetenschappelijke literatuur over de technologieën kwamen enkele thema's telkens terug. Deze thema's – privacy, autonomie, veiligheid, controle over technologie, menselijke waardigheid, rechtvaardigheid en machtsverhoudingen – hebben we gebruikt om de bespreking in dit hoofdstuk te structureren (zie tabel 3.1). De verschillende ethische en maatschappelijke kwesties manifesteren zich per technologisch gebied op verschillende manieren. Privacy krijgt bijvoorbeeld in de context van robotica een andere invulling dan in de context van virtual reality. Niet elk thema wordt bij iedere ontwikkeling uitgediept; we richten ons op de kenmerkende kwesties die een bepaalde technologie laat zien binnen de overkoepelende trend van digitalisering. Tot slot (paragraaf 3.6) vatten we samen welke ethische en maatschappelijke vraagstukken de nieuwe digitaliseringsgolf nadrukkelijk op de kaart zet. We geven kort aan hoe de in dit hoofdstuk gevonden kwesties gerelateerd zijn aan belangrijke waarden zoals die zijn vastgelegd in internationale verdragen. De inzichten over de ethische en maatschappelijke vraagstukken koppelen we aan de inzichten over ontwikkeling van digitalisering uit hoofdstuk 2. Aan de hand van de verschillende fasen in de cybernetische loop – verzamelen, analyseren, en toepassen (zie figuur 2.3 in hoofdstuk 2) – zien we verschillende ethische en maatschappelijke vragen naar voren komen. Dat geeft een beeld van welke kwesties in de komende jaren samenhangen met de ontwikkeling van technologie om aandacht vragen.

**Tabel 3.1** Maatschappelijke en ethische thema's

Thema	Vraagstukken
Privacy	Gegevensbescherming, privacy, digitaal huisrecht, mentale privacy, surveillance, doelverschuiving
Autonomie	Keuzevrijheid, vrijheid van meningsuiting, manipulatie, paternalisme
Veiligheid	Informatieveiligheid, identiteitsfraude, fysieke veiligheid
Controle over technologie	Controle en inzicht in algoritmen, verantwoordelijkheid, onvoorspelbaarheid
Menselijke waardigheid	Dehumanisatie, instrumentalisering, <i>de-skilling</i> , de-socialisatie, werkloosheid
Rechtvaardigheid	Discriminatie, uitsluiting, gelijke behandeling, stigmatisering
Machtsverhoudingen	Oneerlijke concurrentie, uitbuiting, relatie consument-bedrijf

Rathenau Instituut

## Methodiek

Het onderzoek van de beschrijving van de ethische en maatschappelijke kwesties die door de digitalisering worden opgeroepen is uitgevoerd via een literatuurstudie.<sup>19</sup> Per technologiegebied is gezocht naar wetenschappelijke literatuur vanaf 2010 met behulp van zoekmachines zoals Google

<sup>19</sup> Veel dank zijn we verschuldigd aan Luca van der Heide, die de relevante literatuur voor deze literatuurstudie heeft verzameld.



Scholar en Scirus, en met behulp van de PiCarta-database. Per technologiegebied hebben we in combinatie met de term van het technologiegebied (of gerelateerde termen en synoniemen van dit technologiegebied) de volgende zoektermen ingevoerd: ethics, ethical, moral, morality, normative, of normativity. Dit resulteerde ongeveer in zo'n honderd publicaties per technologiegebied. Aan de hand van een eerste screening is dit per technologiegebied gereduceerd tot zo'n twintig à veertig wetenschappelijke publicaties die als meest relevant werden beschouwd voor dit onderzoek. Aan de hand van deze selectie zijn per technologiegebied de belangrijkste ethische en maatschappelijke kwesties beschreven die in de literatuur worden genoemd. De lijst van ethische kwesties is zoals gezegd zeker niet uitputtend, maar toont wel welke ethische kwesties gerelateerd aan de digitalisering van de samenleving kunnen ontstaan en welke als meest urgent en problematisch worden aangemerkt in de wetenschappelijke literatuur. Behalve van wetenschappelijke publicaties is gebruikgemaakt van allerlei kranten en nieuwssites om bepaalde vraagstukken te illustreren aan de hand van aansprekende voorbeelden uit het nieuws.

## 3.2 Materiële wereld

### 3.2.1 Internet of Things

Internet of Things (IoT) is gebaseerd op een wereldwijd netwerk dat de fysieke wereld met de virtuele wereld van het internet integreert. Door de opkomst van het IoT staan we aan het begin van een nieuw tijdperk, waar objecten en mensen in de materiële wereld kunnen worden gemonitord, en waar objecten en mensen automatisch informatie kunnen uitwisselen. Zo kan de wekker niet alleen een persoon wekken maar tegelijkertijd het koffieapparaat aanzetten voor het maken van verse koffie bij het ontbijt, of geeft de koelkast aan wanneer van een product de houdbaarheidsdatum is verstreken, of past de verlichting in de kamer zich aan op wat er gebeurt in een videospel dat er op dat moment gespeeld wordt.<sup>20</sup>

Veel technologiebedrijven verwachten dat IoT in de toekomst alomtegenwoordig zal zijn in ons dagelijks leven. Veel technologieën die we in dit hoofdstuk beschrijven maken in zekere zin deel uit van het IoT. Zo maakt een augmented-reality-bril gebruik van het internet om gebruikers real-time extra informatie te geven over hun omgeving, en kan een biometrische camera gekoppeld zijn aan een online database om gezichten te herkennen.

#### Privacy: digitaal huisrecht

Door IoT worden steeds meer gegevens over ons uitgewisseld, zonder dat we daar echt zicht op hebben of controle over hebben (Barbry 2012; Peppet 2014; Romana et al. 2013). De 46 pagina's tellende privacyhandleiding die behoort bij de slimme tv van Samsung vertelt dat Samsung registreert waar, wanneer, hoe en hoe laat je de tv hebt aanstaan. De tv heeft ook een camera voor gezichtsherkenning en een microfoontje voor spraakherkenning. In de privacyhandleiding waarschuwt Samsung om op te letten voor wat je zegt in de buurt van de tv: 'Please be aware that if your spoken words include personal or other sensitive information, that information will be among

---

<sup>20</sup> [youtube.com/watch?v=1Y3MQrcekrk](https://www.youtube.com/watch?v=1Y3MQrcekrk)

the data captured and transmitted to a third party.' Dit leidde tot aardige ophef (Gibbs 2015). Het voorbeeld laat zien dat er ongewild toestemming wordt gegeven om bepaalde data te gebruiken, omdat mensen niet in staat zijn om de gehele handleiding te begrijpen of omdat last hebben van zogenaamde toestemmingsvermoeidheid (*consent fatigue*) vanwege de grote hoeveelheid toestemmingen die ze moeten geven over het gebruik van data die apparaten opvangen (Pereira, Benessia & Curvelo 2013). Dit roept de vraag op waar de verantwoordelijkheid ligt in dit proces: mag van de gebruiker worden verwacht dat hij van elk apparaat de voorwaarden uitpluist? Of ligt er ook een verantwoordelijkheid bij de producenten van al die apparaten? Zouden zij niet zorg moeten dragen voor een bepaalde redelijke verwachting van privacy.

Door IoT zijn we in feite overal te volgen en dit kan leiden tot een enorme transparantie ten koste van onze privacy. In de meeste gevallen zijn de gegevens die door slimme tandenborstels, thermostaten, televisies, koelkasten en wasmachines worden verzameld eigendom van de producent en niet van de gebruiker. De eigen woning, die we beschouwen als ons privé domein, wordt hierdoor transparant, omdat processen in de woning kunnen worden gemonitord via de IoT-apparaten in de woning. De scheiding tussen huis en buitenwereld vervaagt waarbij de muren en gordijnen het huis niet langer beschermen tegen pottenkijkers. Koops en Prinsen (2005) pleitten er daarom voor burgers te beschermen tegen deze digitale inkijk, en burgers naast fysiek huisrecht ook digitaal huisrecht te geven. Dat zou moeten zorgen voor bescherming tegen waarneming van buitenaf met technische hulpmiddelen, zodat burgers een plaats hebben waar zij 'bij uitstek onbevangen zichzelf kunnen zijn' (Koops & Prinsen 2005, p. 630).

De vraag rijst hoe burgers controle kunnen houden over de datastromen met allerlei persoonlijke gegevens die ontstaan in het IoT. De hoeveelheid gegevens neemt toe, terwijl het maken van een geïnformeerde keuze lastiger wordt omdat veel slimme apparaten functioneren op de achtergrond en niet altijd een makkelijk toegankelijk scherm hebben voor instellingen of privacy notificaties. Een oplossing die wordt genoemd is een digitale privacy assistent; een programma waarin de gebruiker zijn privacyvoorkeuren aangeeft en waarmee de gebruiker de instellingen beter en makkelijker kan managen. Tegelijkertijd zien sommige experts vanuit de industrie en de wetenschap ook dat het bewust uitoefenen van controle over de vele stromen persoonsgegevens in het IoT-tijdperk niet meer praktisch haalbaar is (Eskens et al. 2016). De verantwoordelijkheid voor het managen van de informatiestromen wordt nu vooral bij het individu gelegd, maar er is ook een verschuiving zichtbaar waarbij de verantwoordelijkheid meer bij producenten komt te liggen. Een verantwoorde informatiehuishouding wordt dan onderdeel van het afleveren van een deugdelijk product.

De verantwoordelijkheid van producenten kan bijvoorbeeld gaan over het controleren welke apparaten wel of niet met elkaar mogen communiceren. Een koelkast hoeft bijvoorbeeld niet te communiceren met de auto van de buurman. Een oplossing voor huishoudelijke apparatuur zou kunnen zijn dat deze apparaten alleen met elkaar kunnen communiceren via een gesloten netwerk 'een persoonlijke cloud der dingen'. Een wereldwijd web heb je voor deze apparaten niet echt nodig. Een dergelijke benadering waarbij voor een privacybeschermend ontwerp wordt gekozen, wordt ook wel *privacy by design* genoemd. Daarnaast maakt een perspectief op privacy dat verder gaat dan controle over informatie, het ook mogelijk om na te denken over andere aspecten van privacy, zoals de vrijheid om niet gemonitord te worden en de vrijheid om een eigen identiteit te ontwikkelen (Zureik et al. 2010). Hoe beïnvloedt een slimme TV die continu monitort bijvoorbeeld de

vrije ontwikkeling van meningen en identiteit van de bewoners van het huis? Juist dergelijke vragen komen meer op de voorgrond naarmate zich meer slimme en metende apparaten in onze omgeving nestelen.

### **Autonomie: technologisch paternalisme**

In het IoT komen de drie stappen van de cybernetische loop samen: verzamelen, analyseren en toepassen. Slimme apparaten met sensoren verzamelen data over gedrag (hoe de thermostaat wordt gebruikt), analyseren gegevens via netwerkconnecties (wanneer iemand thuis is en de verwarming aanzet), en zorgen voor een aanpassing (de verwarming springt automatisch aan voordat iemand thuiskomt). Het brein achter IoT bestaat uit de slimme algoritmes die de data in de cloud (big data) analyseren en een beslissing nemen. In een auto bijvoorbeeld kan een sensor zitten die aangeeft dat de brandstof bijna op is. Vervolgens verschijnt op de voorruit van de auto de route naar het dichtstbijzijnde pompstation. Hier is duidelijk sprake van gebruikersgemak, maar ook voor bedrijven – in dit geval brandstofproducenten – is dit type van zeer gerichte marketing lucratief. Het algoritme zou bijvoorbeeld zo ingericht kunnen zijn dat ze de route toont naar de dichtstbijzijnde pomp van het bedrijf dat het meest betaalt aan de ontwerper van het algoritme.

IoT biedt ons niet enkel comfort, maar kan ook neigen naar technologisch paternalisme (Hilty 2015). Van paternalisme is sprake als iemand beter meent te weten wat goed voor anderen is dan deze anderen zelf. Bij technologisch paternalisme wordt het paternalisme ‘gedelegeerd’ aan technologie. Technologisch is het mogelijk dat een slimme koelkast de bestelling van iemands favoriete kaas zelf aanpast door een magere kaas te bestellen omdat de biometrische sensor gemeten heeft dat de cholesterolwaarden van de betreffende persoon te hoog zijn. De vraag is of de koelkast en de biometrische sensor zo’n beslissing wel samen mogen nemen. Dit soort technologisch paternalisme brengt een serieuze ethische kwestie van IoT met zich mee: het impliciet afdwingen of uitlokken van bepaald gedrag kan de persoonlijke autonomie in gevaar brengen. IoT kan zo bovendien als persuasieve of zelfs als manipulatieve technologie ingezet worden (zie subparagraaf 3.2.2 over persuasieve technologie).

Ook wanneer er niet direct sprake is van paternalisme kan de manier waarop een IoT-omgeving ons gedrag beïnvloed onze autonomie inperken. Wanneer een slimme IoT-omgeving op onze wensen en behoeften anticipeert, wordt er een keuze gemaakt over onze veronderstelde voorkeuren – bijvoorbeeld een keuze op bepaalde tv-programma’s voor te stellen – op basis van eerder vertoond gedrag. Met die keuze sorteert de slimme omgeving onze opties voor en stuurt zij aan richting bepaalde keuzes en gedrag. De manier waarop subtiele veranderingen in ons gedrag kunnen worden bewerkstelligd door technologie werd duidelijk in het emotie-experiment van Facebook uit 2014. Door het aantal positieve en negatieve berichten in de *newsfeeds* van gebruikers aan te passen, wisten ze de gemoedstoestand van gebruikers te beïnvloeden zonder dat die zich daarvan bewust waren (Kramer et al. 2014).

Hildebrandt (2012; 2015) stelt dat een toekomstige generatie technologie zo geraffineerd zou kunnen worden in het uitlezen van onze voorkeuren, dat zij preferenties ontdekt voordat wij onszelf daarvan bewust worden. Ze schetst het scenario van een roker die geprofileerd wordt als iemand die bijna wil gaan stoppen, maar nog niet bewust de knoop heeft doorgemaakt en die vervolgens via gerichte advertenties en nieuwsberichten waarin de negatieve effecten van roken worden

bekritiseerd in een andere richting wordt gestuurd. Het verschaffen van transparantie in de profielen waarop automatische beslissingen worden gebaseerd is volgens Hildebrandt een essentiële voorwaarde om de autonomie van het individu te beschermen. De recent aangenomen Europese dataprotectieverordening biedt hiervoor een startpunt, al vormt de uitwerking van de in de verordening opgenomen verordende transparantieplichtingen op een voor de gebruiker betekenisvolle manier nog een grote uitdaging.

### **Veiligheid: informatieveiligheid krijgt een fysieke dimensie**

Digitalisering brengt ook een serieus criminaliteitsprobleem met zich mee: het internet of de apparaten verbonden met het internet zelf kunnen doelwit zijn van criminaliteit, zoals het geval is bij hacken of DDoS (*Distributed Denial of Service*)-aanvallen waarmee websites of systemen worden platgelegd. De ervaring leert dat vrijwel elk digitaal systeem te kraken is. Dat betekent dat kwaadwillenden toegang kunnen krijgen tot gevoelige gegevens, en dat informatie in de handen van de verkeerde personen kan komen. Een gehackte slimme meter zou inbrekers exact inzicht kunnen geven in de tijdstippen in op de dag of week waarop we de verwarming omlaag zetten en – blijkbaar – afwezig zijn. Behalve voor hen waardevolle informatie onttrekken aan slimme apparaten, kunnen criminelen de besturing van slimme apparaten overnemen. Daarmee krijgt het vraagstuk van veiligheid ook een fysieke dimensie. Zo liet een beveiligingsonderzoeker zien hoe eenvoudig de speelgoedpop Cayla is te hacken en hij liet daartoe de pop passages uit de erotische roman *Fifty Shades of Grey* en quotes van de fictieve psychopaat Hannibal Lecter uit het boek *The Silence of the Lambs* citeren.<sup>21</sup> Het hacken van de pop is een relatief onschuldig voorbeeld, maar de Nieuw-Zeelandse hacker Barnaby Jack liet tijdens een conferentie in 2011 zien dat hij de insulinepomp van een vriend te kon hacken. Hij kon de complete bediening overnemen en was in staat een fatale hoeveelheid insuline toe te dienen. Andere hackers lieten ook al zien dat ze de besturing van een via wifi bestuurd pacemaker konden overnemen en het apparaat een fatale schok af konden laten leveren (Greenberg & Zetter 2015). Hiermee werd de angst van voormalig vicepresident van de Verenigde Staten Dick Cheney bewaarheid, die de wifi-functie van zijn pacemaker liet uitschakelen en het apparaat op een alternatieve wijze ging besturen. In Nederland alleen al lopen er duizenden mensen met een vergelijkbare pacemaker met wifi-functie rond, wat de omvang van de gevolgen duidelijk maakt wanneer criminelen zulke apparaten zouden gaan hacken.

Het vraagstuk van beveiliging wordt extra complex doordat in het IoT-apparaten in verbinding met elkaar staan, waardoor een succesvolle hack van een koffiezetapparaat bijvoorbeeld toegang kan verschaffen tot de auto of toegang geven tot de voordeur. Daarnaast zijn dit soort beveiligingsvraagstukken nieuw voor veel producenten van consumentenelektronica, waardoor er niet altijd goed over na wordt gedacht. 'When you put technology on items that haven't had it before, you run into security challenges you haven't thought about before', vat hacker Runa Sandvik het samen (Greenberg & Zetter 2015).

### **Controle: onvoorspelbare netwerkeffecten**

Naast de controle over data is het aspect van controle in relatie tot het IoT op een andere manier relevant. Niet alleen het aantal IoT-apparaten stijgt de komende jaren sterk, ook het aantal

---

<sup>21</sup> [mirror.co.uk/news/technology-science/technology/friend-cayla-doll-can-hacked-5110112](http://mirror.co.uk/news/technology-science/technology/friend-cayla-doll-can-hacked-5110112)

mogelijke interacties tussen deze apparaten onderling neemt toe. Zoals hiervoor beschreven levert dat mogelijk veiligheidsissues op omdat een slecht beveiligd apparaat toegang kan verschaffen tot een ander apparaat. Het levert echter ook onverwachte en onvoorspelbare interactie-effecten op tussen de apparaten zelf. Zo liep het slimme huis van een computerwetenschapper in Berlijn vast – het reageerde op geen enkel commando; lichten, keukenapparatuur en verwarming konden niet meer aan of uit – omdat een van de slimme lampen was doorgebrand en het huis-netwerk had platgelegd door een onophoudelijke stroom berichten te versturen dat de lamp vervangen wilde worden (Hill 2015). Wie er verantwoordelijk is voor de gevolgen van dit soort onverwachte effecten op systeemniveau is bovendien nog onduidelijk (Weber 2011).

### **Machtsverhoudingen: ‘Everything-as-a-service’**

Internet-of-Things-apparaten worden vaak aangeboden als onderdeel van of in combinatie met een software-dienst. Zo wordt een slimme televisie of slimme koelkast in combinatie met software-ondersteuning verkocht. De mogelijkheden van het product liggen voor een belangrijk deel besloten in de bijbehorende software. Zo is de mogelijkheid om de koelkast 's ochtends de agenda voor de komende dag te laten weergeven afhankelijk van de software-ondersteuning van de producent. De producent van het apparaat kan besluiten te stoppen met het aanbieden van ondersteuning voor oudere apparaten, waardoor ze deels of helemaal niet meer werken. De Electronic Frontier Foundation trok aan de bel omdat consumenten die voor honderden dollars een slimme home-console hadden gekocht met levenslange software-ondersteuning, ineens met een waardeloos product zaten omdat de ondersteuning toch geschrapt werd nadat het bedrijf werd overgenomen door een concurrent (Walsh 2015).

Wanneer producten afhankelijker zijn van door de producent beheerde software, versterkt dat de controle die producenten hebben over producten en hoe die gebruikt kunnen worden. Daarnaast is een trend zichtbaar dat producten zelf als dienst worden aangeboden. Dit wordt ‘servitization’ genoemd. Een voorbeeld is dat de consument geen lampen meer koopt, maar licht afneemt als een dienst. Hij schaft geen wasmachine meer aan, maar neemt wassen als een dienst af. De producent is verantwoordelijk voor het onderhoud van de apparaten, de consument hoeft alleen een periodieke vergoeding te betalen. Voorstanders bepleiten het gemak dat dit met zich meebrengt, tegenstanders zien dat de zeggenschap van de consument over de eigen omgeving afneemt; iets zelf openschroeven of aanpassen is bijvoorbeeld niet meer mogelijk. De producent houdt het eigenaarschap en kan ten alle tijden besluiten iets aan het product te wijzigen. Zo besloot Amazon bepaalde eBooks van George Orwell, nota bene de auteur van het boek *1984*, van de eReaders van klanten te verwijderen omdat er een conflict over copyright was met de leverancier. Amazon mocht dat doen, omdat klanten de boeken officieel niet kochten, maar in bruikleen hadden van Amazon (Stone 2009).

### **3.2.2 Robotica**

De ontwikkeling van IoT en robotica zijn sterk met elkaar verbonden. Net als IoT-apparaten zijn robots veelal uitgerust met sensoren om hun omgeving te lezen, zijn ze in toenemende mate verbonden met de cloud om data uit te wisselen en te analyseren, en voeren ze op basis van die analyses zelfstandig acties uit. Hoewel sommige vraagstukken daardoor overlappen brengt robotica ook specifieke ethische dilemma's met zich mee.

### **Privacy: *pervasive monitoring***

Net als het IoT dragen robots bij aan toenemende mogelijkheden tot dataverzameling in situaties waarin voorheen geen (digitale) dataverzameling plaatsvond. Robottechnologieën kunnen op allerlei manieren worden ingezet om bepaalde situaties te monitoren, zoals het wel en wee van patiënten, de gemoedstoestand van een bestuurder van een auto, en de veiligheidssituatie op straat. Als direct gevolg kunnen robottechnologieën op allerlei manieren impact op onze privacy hebben. Zorgrobots en domotica bijvoorbeeld kunnen mensen volgen of de lichamelijke gesteldheid van mensen vastleggen en doorgeven, en maken het zelfs mogelijk dat er 24 uur per dag wordt meegekeken met de zorgontvanger. Deze data geven veel informatie over het dagelijks reilen en zeilen van de zorgontvangers en werpen daardoor vragen op over hun privacy. Zorgontvangers zullen het bijvoorbeeld niet prettig vinden dat wordt vastgelegd wanneer ze nog niet aangekleed zijn of juist in bad gaan. Deze kwestie wordt complexer als het gaat om dementerende ouderen: in hoeverre kunnen zij aangeven of zij zich bewust zijn van de aanwezigheid van een technologie die hun dagelijks leven vastlegt (Borenstein & Pearson 2010)?

Een ander belangrijk issue in relatie tot privacy dat veelvuldig terugkomt bij digitalisering betreft de mogelijkheid dat technologie voor een ander doel wordt ingezet dan oorspronkelijk bedoeld is. Men spreekt ook wel van doelverschuiving of in het Engels van *function creep*. Dat zien we bijvoorbeeld bij de digitalisering en robotisering van de auto. De Europese Commissie heeft het eCall-systeem – een systeem dat automatisch hulpdiensten alarmeert bij een ongeval – verplicht gesteld voor personenauto's die vanaf 2018 verkocht worden. Het Europese Parlement heeft geëist dat dit eCall-systeem een 'slapend bestaan' leidt en pas in actie komt zodra er een ongeluk plaatsvindt. Dit systeem kan dus niet ingezet worden voor het opsporen van criminelen. Doelverschuiving ligt echter steeds op de loer. De vraag is namelijk of dergelijke mogelijkheden in de toekomst niet toch ook ingezet zullen worden om data te verzamelen voor de opsporing of het voor het handhaven van de (verkeers)veiligheid. Zo werd bijvoorbeeld in 2011 bekend dat de camera's die toezicht hielden op vervuillende vrachtwagens binnen Amsterdam ook gebruikt zouden worden om te zien of eigenaren van kentekens iets op hun kerfstok hadden of nog een boete moesten betalen. Volgens Het Parool ging hiermee een langgekoesterde wens van de toenmalige hoofdcommissaris Bernard Welten in vervulling: de realisatie van een 'digitale slotgracht' rond de stad.<sup>22</sup>

### **Autonomie: 'man out-of-the-loop'**

In de robotica zien we een verschuiving 'from *in-the-loop* to *on-the-loop* to *out-the-loop*' (Sharkey 2010), welke ook merkbaar is in IoT. 'In the loop' betekent dat de mens in controle is en menselijke toestemming nodig is om het systeem een actie uit te laten voeren. 'On the loop' houdt in dat de mens een beslissing maakt op basis van informatie van het systeem. 'Out of the loop' verwijst naar een situatie van volledige automatisering, waarbij het systeem zonder menselijke tussenkomst een beslissing neemt. De verschuiving van *in* naar *on* en *out the loop* wordt in de hand gewerkt door de toename van de hoeveelheid informatie van verschillende bronnen/apparaten die moet worden geïntegreerd en vervolgens moet worden geïnterpreteerd om tot een beslissing te komen. Robots kunnen dit veel efficiënter en effectiever dan mensen, voor wie het haast ondoenlijk is. Dit heeft tot gevolg dat mensen in feite zelf niet meer de beslissingen nemen maar dat overlaten aan

---

<sup>22</sup> Het Parool (7 september 2011), Digitale ring scant alle auto's.

technologie. Voorbeelden zijn kennissystemen die medische diagnoses stellen aan de hand van een grote hoeveelheid informatie, militaire robots die beslissen over leven en dood op basis van informatie vanuit verschillende bronnen en rijtaakondersteunende systemen die bijvoorbeeld beslissen welke snelheid we op een bepaald stuk weg moeten rijden. Het roept de vraag op hoe deze systemen tot hun beslissingen komen en of de software van de concurrent dezelfde beslissing zou nemen.

Ethische vragen die met betrekking tot autonomie een antwoord behoeven zijn: in welke omstandigheden en in hoeverre mag de persoonlijke autonomie van mensen aangetast worden? Waar blijft de ruimte voor eigen beslissingen? En welke consequenties heeft de aantasting van de persoonlijke autonomie op de rol van de eigen verantwoordelijkheid van mensen? Wat dit laatste betreft, zijn mensen geneigd op de technologie te vertrouwen en daar blind op te varen. Maar wat nu als de technologie faalt – er wordt bijvoorbeeld geen signaal afgegeven als de auto de muur bijna raakt en het gaat mis – wie is daar dan voor aansprakelijk?

Door de sterke progressie in kunstmatige intelligentie worden robots steeds autonomer. De vraag die rijst is in hoeverre het ethisch aanvaardbaar is om de verantwoordelijkheid om morele beslissingen te nemen over te laten aan robots. De discussie speelt al in het gebied van militaire robots en zelfrijdende auto's. Volgens Arkin (2010) gaat de militaire robot de menselijke militair overtreffen bij het nemen van morele beslissingen, omdat menselijke militairen enorme stress ondervinden op het slagveld, en robots – vrij van stress – minder fouten maken. Het probleem hierbij is dat robots niet ter verantwoording kunnen worden geroepen, en dat is voor veel wetenschappers de reden dat robots nooit over leven en dood mogen beslissen.<sup>23</sup>

Het zelfde probleem doet zich voor bij zelfrijdende auto's. Verkeersongevallen zijn, ook met zelfrijdende auto's, onvermijdelijk, en dus zal zo'n auto in situaties terecht komen die een morele beslissing vereisen (Goodall 2014). Een mens handelt in zo'n situatie uit een reflex; je kunt onmogelijk verwachten dat hij in een halve seconde een weloverwogen keuze maakt tussen zelf tegen een vrachtwagen aan te rijden of een kind op de stoep omver rijden. Voor een zelfrijdende auto is een halve seconde echter ruim voldoende om verschillende scenario's door te rekenen. Moet de auto kiezen voor de minste schade voor de inzittenden in die auto of bijvoorbeeld voor de minst totale schade waarbij dus ook rekening wordt gehouden met andere verkeersdeelnemers? De vraag die aan deze kwestie vooraf gaat, is: laten we deze morele beslissing over aan de zelfrijdende auto, of bepalen we van tevoren wat deze auto moet beslissen in het geval dat de auto een ongeluk niet kan vermijden? Ook hier zullen veel mensen geneigd zijn die keuze niet aan een apparaat over te laten, maar deze keuze over te laten aan de mens omdat het ook hier gaat over leven en dood. Dat leidt tot de volgende vraag: wie moet de beslissing dan nemen over hoe de zelfrijdende auto zich in dit soort situaties moet 'gedragen'? De consument, de overheid, de

---

<sup>23</sup> In 2010 werd tijdens de expertworkshop Limiting Armed Tele-Operated and Autonomous Systems, georganiseerd door International Committee for Robot Arms Control (ICRAC), een verklaring ondertekend door een grote meerderheid van de aanwezigen waarin de noodzaak tot beperking van bewapende militaire robots en een verbod op autonome bewapende militaire robots worden benadrukt, met als achterliggende gedachte dat altijd een mens de beslissing moet nemen over leven en dood ([icrac.co.uk/Expert%20Workshop%20Statement.pdf](http://icrac.co.uk/Expert%20Workshop%20Statement.pdf)). Zie ook de open brief van meer dan duizenden deskundigen inzake AI en robotica uit 2015 ([futureoflife.org/open-letter-autonomous-weapons](http://futureoflife.org/open-letter-autonomous-weapons)).

ontwerper, of de fabrikant? Dit complex van vragen zal zeker beantwoord moeten worden voordat zelfrijdende auto's voor de consument beschikbaar zijn.

### **Veiligheid: hacken van robotica**

Net als bij het Internet of Things maakt robotica duidelijk dat digitale veiligheid een fysieke dimensie krijgt. De digitalisering van de auto maakt de auto kwetsbaar voor hacken. Virussen kunnen auto's zo ontregelen dat ze onbestuurbaar worden en ongewenste acties gaan uitvoeren. Door het 'kraken' van de auto is het zelfs mogelijk om volledige controle over de auto te krijgen. Hetzelfde verhaal geldt wellicht nog in sterkere mate voor militaire en politie-drones. In 2012 bijvoorbeeld, hebben onderzoekers van de Universiteit van Texas in opdracht van het ministerie voor Binnenlandse Veiligheid laten zien hoe relatief eenvoudig het was om de besturing van een drone over te nemen.<sup>24</sup> Ze gebruikten daarvoor de techniek die bekend staat als *spoofing*: het ongeautoriseerd toegang verkrijgen tot een apparaat door middel van het vervalsen van de identiteit van diegene die het apparaat bestuurt. In beleidskringen heerst dan ook de vrees voor cyberterrorisme.

### **Menselijke waardigheid: morele plicht tot robotisering, dehumanisering en werkeloosheid**

Een kernvraag bij ontwikkeling van robotica is wanneer we haar in willen zetten. De inzet van robots kan een bijdrage leveren aan menselijk welzijn, maar kan ook tot dehumaniserende situaties leiden.

De positieve bijdrage die robotica kan leveren ligt bijvoorbeeld in de mogelijkheid dat robots 'smerig, saai en gevaarlijk' (*dirty, dull & dangerous*) werk kunnen overnemen. Bepaalde taken kunnen inderdaad zo smerig, geestdodend of gevaarlijk zijn dat het onwenselijk is om dergelijke taken door mensen uit te laten voeren als het ook mogelijk is om dat door een machine te laten doen. Strawser (2013) vindt het bijvoorbeeld moreel verwerpelijk om een militair een bevel te geven waarbij hij de kans loopt op dodelijk letsel als een militaire robot die taak ook had kunnen uitvoeren. Dit 'principe van onnodig risico' leidt tot een ethische verplichting om robotica in bepaalde situaties toe te passen, bijvoorbeeld bij het zoeken naar en ontmantelen van bembommen. Prostitutie is in Nederland sinds 2000 legaal, maar het blijkt veelal een smerig, gevaarlijk en mensonterend beroep te zijn (Werson 2012). Volgens het Korps Landelijke Politiediensten werkt tussen de vijftig en negentig procent van de 25.000 vrouwen in de prostitutie in Nederland onvrijwillig (KLPD 2008). Het is een actuele vraag hoe de politiek dergelijke grove en voor de betreffende vrouwen traumatische menselijke misstanden tegen kan gaan. De opkomst van de nieuwe robotica brengt een nieuw perspectief in deze discussie. Ze agendeert namelijk de vraag of seksrobots op termijn een redelijk alternatief kunnen vormen voor menselijke prostitutie. Een volgende stap is dan, bij aanwezigheid van zo'n alternatief, of er gelet op de vele mensonwaardige omstandigheden in de prostitutie dan niet een ethische verplichting moet komen om seksrobots toe te passen.

Het 'principe van onnodig risico' is van toepassing op verschillende gebieden (Royakkers & Van Est 2015). Robotica biedt tal van mogelijkheden om de veiligheid van het huidige verkeerssysteem te verbeteren. Dat geldt onder meer voor het reeds bestaande ISA-systeem. Deze intelligente

---

<sup>24</sup> [bbc.com/news/technology-18643134](http://bbc.com/news/technology-18643134)



snelheidsassistent geeft informatie over de snelheidslimiet en waarschuwt of grijpt in bij snelheidsovertredingen. Het verplicht stellen van de ingrijpende variant van het ISA-systeem kan volgens experts bijdragen tot een halvering van het totaal aantal verkeersdoden in Europa. In 2014 kwamen bijna 26 duizend mensen om in het verkeer.<sup>25</sup> Hier legt de nieuwe robotica duidelijk de vraag op tafel of we niet moreel verplicht zijn om automatische snelheidsbegrenzing in auto's wettelijk verplicht te stellen. Hoewel dit een inperking zou zijn van de individuele autonomie zou de afweging kunnen worden gemaakt dat deze inperking te rechtvaardigen is door de reductie in het aantal verkeersslachtoffers. Een andere toepassing zou bijvoorbeeld medische operaties kunnen zijn. Met een operatierobot, zoals de Da Vinci-robot, kunnen artsen veel nauwkeurigere en minder belastende ingrepen uitvoeren.<sup>26</sup>

De negatieve kant van robotisering komt vooral naar voren wanneer de inzet van robotica leidt tot dehumanisering. De toepassing van robotica op de terreinen van de zorg, amusement, politie en het leger kan zorgen voor belangrijke ondersteuning, maar kan wanneer de technologie niet binnen bepaalde randvoorwaarden wordt ingezet ook de menselijke waardigheid ondermijnen. Het gaat om het gevaar van objectivering of instrumentalisering van mensen, oftewel dehumanisering. Met name met betrekking tot de inzet van robotica in de zorg bestaat hier angst voor. De manier waarop robots ingezet worden, lijkt hierbij een cruciaal punt. Coeckelberg (2010) stelt dat zorgrobots slechts mogen worden ingezet voor 'routinematige zorgklussen'. Het gaat dan om taken waarbij geen emotionele, intieme, persoonlijke betrokkenheid vereist is. Het zorgzaam zijn – '*care giving*' – is voorbehouden aan mensen. Wanneer robots worden ingezet ter vervanging van de verzorger, bestaat het risico dat zorg gedehumaniseerd wordt (Sharkey 2014). Wanneer robots taken zoals voeden en optillen overnemen, kunnen de zorgvragers zich als objecten voelen. Sterker nog, ze zien de mogelijkheid dat ouderen hierdoor het idee hebben minder controle over hun leven te hebben dan wanneer ze zorg van verzorgers ontvangen. Het ethische bezwaar van 'objectivering van de patiënt' sluit aan bij de gedachte dat robots niet kunnen zorgen. Robots zijn apparaten die de empathische capaciteiten en wederkerigheid van menselijke zorgrelaties niet kunnen repliceren, is de onderbouwing. Menselijk contact wordt vaak als noodzakelijk gezien voor het verlenen van goede zorg. Kwaliteit van leven van de patiënt dient dan ook het leidende principe te zijn bij robotica in de zorg.

Ook in andere gebieden van de zorg is er een risico op dehumanisering. Militairen of politieagenten die robots op afstand besturen, zijn niet aanwezig in de betreffende gevarezone. De inzet van telegeleide robots zorgt zodoende voor een emotionele, en daardoor ook morele afstand tussen de actie en de ethische implicaties van die actie. Voorstanders stellen dat dit tot minder psychologisch leed onder militairen leidt en tot rationelere besluiten kan leiden. Critici vrezen dat in het creëren van meer afstand tussen een handeling en de gevolgen ervan het gevaar schuilt dat bestuurders belangrijke beslissingen, soms over leven en dood, nemen alsof ze een videospelletje spelen. Daarnaast zijn de bestuurders voor het maken van hun beslissingen afhankelijk van de beperkte informatie die door de robot wordt verstrekt. Bij de inzet van telegeleide bewapende robots bestaat zodoende het gevaar van dehumanisering van de vijand, en van de afstomping van de bestuurder.

---

<sup>25</sup> [ec.europa.eu/transport/road\\_safety/pdf/observatory/trends\\_figures.pdf](http://ec.europa.eu/transport/road_safety/pdf/observatory/trends_figures.pdf)

<sup>26</sup> [erasmusmc.nl/davincirobot/DaVinciRobot](http://erasmusmc.nl/davincirobot/DaVinciRobot)

Een ander aspect dat de afgelopen jaren tot veel discussie heeft geleid is het mogelijke effect van robotisering op de werkgelegenheid. Robots kunnen niet alleen worden ingezet ter ondersteuning van menselijke taken, ze kunnen gaandeweg ook steeds meer menselijke taken vervangen en dus ook arbeidsplaatsen invullen. Twee tegengestelde visies domineren deze discussie over de invloed van de robotisering. Enerzijds is er de visie dat robotisering leidt tot economische groei, banengroei (er worden nieuwe banen gecreëerd) en een acceptabele verdeling van de welvaart, en anderzijds de visie dat robotisering tot minder werk leidt met als gevolg een krimpende welvaart.<sup>27</sup> Het behouden van menselijke waardigheid is cruciaal voor de maatschappelijke acceptatie van de nieuwe robotica. Robotica kan een belangrijke rol spelen in het versterken van menselijk welzijn, maar dat betekent ook dat er moet worden nagedacht over de manier waarop menselijke waardigheid wordt beschermd. De ontwikkelingen in robotica laten zien dat deze vraagstukken niet alleen op de lange termijn gaan spelen maar ons nu al dwingen te reflecteren op de huidige ontstane praktijk.

### 3.3 Biologische wereld

#### 3.3.1 Biometrie

Het gebruik van biometrische informatie betekent dat unieke lichamelijke kernmerken –zoals het gelaat, de stem of de vingerafdruk – van een persoon worden gebruikt voor verificatie of identificatie. Een voorbeeld van verificatie door middel van biometrie zijn de elektronische grenspassage-poorten (e-gates) op vliegvelden. De reiziger legt zijn paspoort op een lezer, kijkt in de camera en het poortje gaat al of niet open. Het identificatiesysteem doet hierbij het volgende: een digitaal beeld van het gezicht, opgeslagen in het paspoort, wordt vergeleken met de opname van het gezicht die gemaakt is toen de reiziger in de camera keek. Als het biometrische systeem – in dit geval een gezichtsherkenner – beslist dat het gezicht opgeslagen in het paspoort van dezelfde persoon afkomstig is als de actuele opname, dan concludeert het paspoortcontrolesysteem dat hij de rechtmatige eigenaar van het paspoort moet zijn en opent de e-gate.

#### **Privacy: *privacy enhancing* versus verlies van controle over gevoelige informatie**

Biometrische technologie is een tweezijdig zwaard in relatie tot privacy. Het kan op een privacybeschermende manier worden ingezet waarbij alleen de minimaal nodige informatie wordt gebruikt om bijvoorbeeld te bepalen of iemand gerechtigd is om een gebouw binnen te gaan of alcohol te kopen. Aan de andere kant is het gebruik van biometrie gevoelig, en kan controle over wat er met die informatie gebeurt lastig zijn, zeker nu de ontwikkeling van de technologie op een fase is beland dat zij in veel meer apparaten en situaties kan worden toegepast.

In het hierboven beschreven voorbeeld van de e-gates wordt biometrie ingezet op een manier waarop de privacy wordt gewaarborgd. De identiteit van de gebruiker wordt namelijk niet vrijgegeven, maar er vindt alleen verificatie plaats: is het gezicht voor de camera hetzelfde gezicht

---

<sup>27</sup> Zie voor een uitvoerige studie over dit onderwerp: Van Est & Kool (2015).

als op het paspoort staat? Verificatie kan ook door een biometrische eigenschap van een persoon te vergelijken met de informatie die reeds over die persoon is opgeslagen. Bijvoorbeeld als een slijter van een biometrisch systeem gebruik maakt van vingerafdrukken om te verifiëren dat iemand ouder is dan achttien jaar, hoeft hij alleen te weten dat bij die vingerafdruk de informatie hoort dat diegene ouder dan achttien jaar is. De naam van de klant is niet van belang. Biometrie kan dus een mooi middel zijn om legitimiteit aan te tonen met behoud van privacy.

Andere toepassingen van biometrie richten zich juist wel op identificatie. Bijvoorbeeld door het gezichtsprofiel van iemand te vergelijken met een databank om te zien of de gescande persoon in de databank voorkomt. Dit wordt toegepast bij bijvoorbeeld opsporing door de politie of bij de beveiliging van publieke ruimtes door middel van camera's. Dit gebruik is bij wet geregeld. Van belang is een veilige en beschermde opslag van deze zeer gevoelige informatie. Biometrische gegevens kunnen namelijk informatie bevatten over bijvoorbeeld de gezondheid en de etniciteit van de gebruiker (Juul 2013). Het kan onwenselijk zijn dat deze gegevens in handen komen van bijvoorbeeld een verzekeringsmaatschappij of een werkgever. Dit probleem wordt verergerd doordat de moderne biometrische identificatiemethoden ook aanwijzingen kunnen vinden voor bijvoorbeeld de gezondheidsrisico's van een persoon. Op basis van bijvoorbeeld een irisscan kan diabetes of een hoge bloeddruk worden vastgesteld. Onregelmatigheden in de vingerafdrukken kunnen duiden op leukemie of borstkanker.

Om privacyrisico's van biometrie te voorkomen is het volgens Veldhuis (2015) van groot belang om biometrische gegevens zo op te slaan dat ze wel gebruikt kunnen worden voor herkenning, maar geen informatie over het onderliggende biometrische kenmerk prijsgeven. Technische oplossingen zoals *biometric template recognition*<sup>28</sup> en slimme cryptografische versleuteling kunnen hiervoor een oplossing bieden. Tegelijkertijd liggen doelverschuiving en het oneigenlijk gebruik van gegevens wel op de loer als het gaat om biometrie. Bij doelbinding met betrekking tot biometrie gaat het erom of de biometrische gegevens adequaat, relevant en proportioneel zijn in relatie tot het doel waarvoor ze zijn verzameld. In het verleden zijn er al voorbeelden dat hier niet altijd aan wordt voldaan (Renaud, Hoskins & Von Solms 2015). In een nachtclub in Glasgow bijvoorbeeld gebruikte het personeel een vingerafdruklezer om de leeftijd en identiteit van hun klanten te verifiëren. Dit om zogenaamd het alcoholprobleem in de stad terug te dringen. Achteraf bleek echter dat dit werd gedaan voor het gemak van de uitsmijters en om meer winst te maken via profiling op basis van de identiteit van de klanten.

In de afgelopen jaren heeft biometrie een sterke ontwikkeling doorgemaakt. De aanwezigheid van grote databases met foto's, de toegankelijkheid van software, en alomtegenwoordigheid van camera's in smartphones, zorgen ervoor dat gezichtsherkenningstechnologie in steeds meer situaties kan worden toegepast (Jansen et al. 2015). Wetenschappers lieten zien dat ze met behulp van gezichtsherkenningstechnologie en openbare data van Facebook profielen op een universiteitscampus een derde van de studenten konden identificeren (Acquisti et al. 2014). De

---

<sup>28</sup> Bij *biometric template recognition* wordt alleen een profiel van de afstanden tussen verschillende gezichtskenmerken gebruikt zonder dat het originele beeld opgeslagen hoeft te worden. Het template kan daarmee losgekoppeld worden van identificerende gegevens van een individu (Veldhuis 2010).

vrees is dat toegankelijke gezichtsherkenningstechnologie uiteindelijk kan leiden tot een situatie waarin het niet meer mogelijk is om anoniem over straat te gaan. In Rusland werd in 2016 de app FindFace gelanceerd, waarmee gebruikers een foto die ze bijvoorbeeld van iemand op straat hebben gemaakt, kunnen vergelijken met profielfoto's op Vkontakte – de Russische tegenhanger van Facebook – om zo iemands identiteit te achterhalen. 'If you see someone you like, you can photograph them, find their identity, and then send them a friend request', aldus een van de makers van de app (Walker 2016).

Een volgende generatie biometrie geeft bovendien niet alleen inzicht in 'wie u bent', maar richt zich ook op de vraag 'hoe u zich voelt' (Mordine, Tzovaras & Ashton 2012).

Emotieherkenningstechnologie geeft bijvoorbeeld inzicht in de gemoedstoestand van mensen, en kan zelfs worden ingezet om emoties die mensen proberen te verhullen, bloot te leggen door te kijken naar onbewuste automatische non-verbale reacties van mensen (Dwoskin & Rusli 2015). Het gaat hier om inbreuk op een nieuw terrein van de privacy, namelijk de 'mentale privacy'. Dat wil zeggen het recht en het vermogen van mensen om privé te houden wat ze denken en voelen. Naast gezichtsuitdrukkingen kunnen ook andere vormen van gedrag worden geanalyseerd. Zo kunnen bepaalde manieren van lopen, grimassen en gezichtsuitdrukkingen, iets blootgeven over een persoon en zijn gedrag. De mate waarin een persoon controle heeft over het al dan niet afgeven van bovengenoemde gegevens lijkt beperkt, aangezien het verzamelen van deze informatie op afstand en verborgen kan plaatsvinden – bijvoorbeeld door gezichtsherkenningstechnologie in te bouwen in paspoppen<sup>29</sup> – zonder medeweten van de persoon die geobserveerd wordt (De Hert & Sprokkereef 2012).

### **Veiligheid: identiteitsfraude**

Uit onderzoek van PWC (2013) blijkt dat identiteitsfraude een groot maatschappelijk probleem is dat in omvang waarschijnlijk alleen maar toeneemt. Identiteitsfraude is het opzettelijk verkrijgen, toe-eigenen, bezitten of creëren van valse identificatiemiddelen en het daarmee begaan van een wederrechtelijke gedraging of met de intentie om daarmee een wederrechtelijke gedraging te begaan. Geavanceerde biometrie moet identiteitsfraude terugdringen. Paspooten zijn tegenwoordig voorzien van een chip met gelaatsscan en digitale vingerafdrukken. In het Verenigd Koninkrijk wordt daarnaast ook een irisscan gemaakt. Biometrische herkenning heeft naast het veel genoemde gebruikersgemak, vanuit veiligheidsoogpunt ook als voordeel dat de gebruiker fysiek aanwezig moet zijn. Daarmee wordt de kans op fraude door middel van vervalsing van documenten, diefstal van pasjes en het ontfutselen van wachtwoorden kleiner.

Hoewel biometrie voordelen biedt ten opzichte van wachtwoorden, pincodes, magneetstrips, et cetera, zijn er ook significante nadelen. Zoals we al geconstateerd hebben gaat het hier om zeer gevoelige informatie die niet in verkeerde handen moet komen. En ook biometrische technologie is niet onfeilbaar (Heimo et al. 2012): biometrische systemen kunnen misleid worden met vervalste kenmerken, bijvoorbeeld door middel van spoofing: het vervalsen van kenmerken met als doel om tijdelijk een valse identiteit aan te nemen. Zo lieten Duitse hackers zien dat ze met behulp van een paar foto's – onder andere van een persconferentie – de vingerafdruk van de Duitse minister van

---

<sup>29</sup> [wired.co.uk/news/archive/2012-11/23/mannequin-spies-on-customers](http://wired.co.uk/news/archive/2012-11/23/mannequin-spies-on-customers)

Defensie konden namaken (Hern 2014). Extra nadelig is dat we in het geval van biometrische identiteitsfraude geen andere vingerafdruk of gezichtsprofiel kunnen nemen zoals we wel een nieuw wachtwoord aan kunnen vragen. Ook leidden minder geraffineerde methoden van identiteitsfraude al tot de eerste horrorscenario's bij beveiliging met vingerafdrukken. Bij een auto die was uitgerust met een vingerafdruklezer om de beveiliging uit te schakelen, werd tijdens een autodiefstal de vinger van de eigenaar afgesneden, zodat de daders met de auto weg konden rijden.<sup>30</sup>

### **Menselijke waardigheid: instrumentalisering en de standaardmens**

Zoals hiervoor ook aangegeven zijn biometrische systemen niet onfeilbaar. Ze kunnen zowel 'vals negatieve' als 'vals positieve' resultaten geven. Een 'vals negatief' resultaat krijg je als het identificatieapparaat een gerechtigd persoon niet herkent. Dit hoeft niet direct een probleem te zijn als de persoon zich maar onmiddellijk opnieuw kan proberen te identificeren. Maar iets dergelijks kan ook voor behoorlijk wat ongemak zorgen. Zo werd in de Verenigde Staten een automobilist zijn rijbewijs afgenomen, omdat het gezichtsherkenningssysteem hem aanzag voor een ander. Na tien dagen bureaucratisch geworstel waarin hij bewees dat hij was wie hij was kreeg hij uiteindelijk zijn rijbewijs terug.<sup>31</sup> Dit voorbeeld laat zien dat het gebruik van biometrische systemen kan leiden tot instrumentalisering van het individu, waarbij het individu wordt gereduceerd tot een datapunt in een systeem. Het gebruiksgemak van biometrie is groot voor degene voor wie het systeem goed functioneert. Maar voor wie ten onrechte door het systeem wordt aangeduid als verdacht is het vaak zeer lastig om fouten recht te zetten. Daarnaast blijkt biometrie niet voor alle mensen inzetbaar. Zo heeft vanwege ouderdom of bepaalde chemotherapie twee procent van de mensen geen vingerafdruk die 'gelezen' kan worden (Renaud, Hoskins & Von Solms 2015). Een dergelijk probleem speelt bij veel digitale systemen: de systemen zijn ontworpen op basis van de kenmerken van een bepaald standaard type gebruiker, waarmee ze niet altijd toegankelijk zijn voor mensen die niet aan die eigenschappen voldoen, bijvoorbeeld omdat ze een naam hebben die niet in het systeem past, of van geslacht zijn veranderd.

### **Rechtvaardigheid: classificatie en het vermoeden van onschuld**

De toepassing van biometrie kan leiden tot verkeerde classificatie en stigmatisering, door een persoon automatisch in een bepaalde categorie te plaatsen, zoals terrorist, crimineel of onbetrouwbaar individu. Dit kan leiden tot een omkering van het vermoeden van onschuld. Door deze biometrische systemen kan iemand immers als crimineel beschouwd worden totdat het bewijs van het tegendeel is geleverd. De kans is groot dat deze stigmatisering aan zo'n persoon blijft kleven, bijvoorbeeld doordat het vermoeden wordt opgeslagen in een databank (Sutrop & Laas-Mikko 2012; Sutrop 2010). Dit kan nog eens versterkt worden door gezichtsherkenning, waardoor de identiteit van een persoon makkelijk is te achterhalen. De stigmatisering van een persoon kan dus plaatsvinden zonder dat die persoon hier weet van heeft. In naam van de nationale veiligheid, is de stap naar doelverschuiving klein.

---

<sup>30</sup> [news.bbc.co.uk/2/hi/asia-pacific/4396831.stm](http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm)

<sup>31</sup> [schneier.com/crypto-gram/archives/2011/0815](http://schneier.com/crypto-gram/archives/2011/0815)

### 3.3.2 Persuasieve technologie

Persuasieve technologie wordt door Fogg (2002) gedefinieerd als technologie die als doel heeft om mensen aan te zetten tot het veranderen van hun gedrag. Om dit te bewerkstelligen moet er volgens Fogg (2002) sprake zijn van een juiste motivatie, de mogelijkheid om actie te ondernemen en een prikkel die aanzet tot een bepaald gedrag. Persuasieve technologie wordt bijvoorbeeld ingezet worden om een automobilist over te halen een autogordel te dragen. Veiligheid is hier de motivatie. Door een signaal te laten horen wanneer de bestuurder de autogordel niet om heeft, kan deze verleid worden de gordel daadwerkelijk om te doen.

#### **Autonomie: sturing en manipulatie door technologie**

De meest prominente ethische vraag die zich bij persuasieve technologie opdringt is die van de menselijke autonomie: in hoeverre mogen we mensen beïnvloeden en wanneer mogen we deze technologie inzetten? Volgens Smids (2012) behoort persuasieve technologie te voldoen aan de eis van vrijwilligheid om autonomie te garanderen. Een handeling wordt uitsluitend vrijwillig gedaan als de handeling intentioneel wordt gedaan (diegene die handelt is 'in control') en vrij is van controlerende invloeden. Als iemand bijvoorbeeld de autogordel niet wil dragen en hierdoor een constant piepend geluid hoort, dan wordt diegene onderworpen aan een controlerende invloed – in dit geval een soort van dwang. De bestuurder kan het irriterend geluid alleen opheffen door het dragen van de gordel. Naast dwang, zoals hier, zijn voorbeelden van controlerende invloeden manipulatie (bijvoorbeeld het achterhouden van informatie of misleiding) en buitensporige stimuli (bijvoorbeeld een heel grote beloning).

Idealiter is het doel van persuasieve technologie dat de verleiding stopt, en dat de gebruiker zelfstandig het 'gewenste' gedrag vertoont. In dat geval leidt persuasieve technologie de gebruiker op. Het doel van iemand opleiden is dat hij zelfstandig kan functioneren en dat hij geen begeleiding meer hoeft. In tegenstelling tot opleiden, is het doel van manipuleren om iemand afhankelijk te houden. Volgens Spahn (2012) moet persuasieve technologie opleiden en niet manipuleren, en zichzelf uiteindelijk overbodig maken. Een belangrijke voorwaarde hiervoor is dat de gebruiker het doel van de beoogde verleiding deelt. Als een gebruiker duurzamer wil rijden dan zal hij elke poging om hem te helpen zijn doel te bereiken van harte omarmen. Als de gebruiker het doel niet deelt, dan kan een aanvullende motivering een oplossing bieden, in dit voorbeeld door te wijzen dat het financieel aantrekkelijk is om duurzaam te rijden.

Technologie die op een meer dwingende manier het gedrag stuurt, is echter niet per definitie onwenselijk. Ten eerste kunnen mensen er zelf voor kiezen om dwingende technologieën in te zetten. Zo kunnen mensen zeer tevreden zijn met het piepgeluid dat een auto geeft als ze te dicht op een ander voertuig of object rijden bij bijvoorbeeld het inparkeren, of met pauzesoftware voor het tegengaan van RSI met programma's waarin de pauzes dwingend zijn. Mensen kiezen er dan zelf voor, door deze systemen niet uit te zetten, om afhankelijk te zijn van deze technologie. Ten tweede kunnen dwingende technologieën ingezet worden als het gedrag van het individu leidt tot een collectief risico. Zo zijn er voorstanders voor verplichte snelheidsbegrenzers op auto's, die de individuele vrijheid inperken, maar het collectieve risico van andere verkeersdeelnemers terugbrengen. Ten derde kan technologie worden ingezet om mensen te weerhouden van

gedragingen die per definitie een gevaar vormen voor anderen, zoals met te veel drank op een auto willen besturen. Het alcoholslot zou vanuit dat argument ethisch gezien verdedigbaar zijn.

Persuasieve technologie kan zoals we eerder zagen ook een onderdeel vormen van slimme Internet-of-Things-omgevingen. Dat betekent dat beïnvloeding onderdeel wordt van de omgeving en in sommige gevallen minder bewust plaatsvindt. Dit is bijvoorbeeld het geval wanneer gebruik wordt gemaakt van subtiele lichtfeedback (Maan et al. 2011), waarbij beïnvloeding op een laag-cognitief niveau plaatsvindt zonder dat de gebruiker zich daarvan bewust is. Dergelijke vormen van beïnvloeding kunnen een bedreiging vormen voor de autonomie van het individu, wanneer het gedrag wordt gestuurd zonder medeweten of zonder dat het individu zich er bewust van is. Transparantie en inzicht in de manier waarop persuasieve technologie wordt ingezet zijn dan ook van belang om de autonomie te beschermen (Compen et al. 2014).

### **Menselijke waardigheid: afleren van morele vaardigheden**

Een bezwaar tegen persuasieve technologie is dat het handelen van gebruikers niets meer met ethiek te maken heeft: ze maken geen morele keuze maar vertonen simpelweg gestuurd gedrag (Spahn 2013). Een rijtaakondersteunend systeem dat ons constant waarschuwt dat we te snel rijden kan qua veiligheid zeer effectief zijn, maar het risico is een zekere verschraling van het normbewustzijn. Persuasieve technologie is potentieel een krachtig reguleringsinstrument, maar de morele vraagstukken vragen om een nadere overdenking van de inzet van persuasieve technologie als technisch reguleringsinstrument. Het doembeeld van critici is dat persuasieve technologie leidt tot een samenleving waarin burgers gestuurd worden tot normconform handelen zonder dat zij de norm zelf nog voelen. Internet criticus Morozov (2013) pleit daarom voor technologie die het deliberatieve vermogen van mensen (het vermogen om informatie te vergaren en met andere mensen te overleggen en argumenten uit te wisselen) stimuleert, aanzet tot reflectie en van daaruit eventueel leidt tot gedragsverandering. Een wasmachine kan een gebruiker met een feedbackmechanisme stimuleren op een energiezuinige, lagere temperatuur te wassen, maar de gebruiker denkt daarmee niet vanzelfsprekend na over de vraag of hij überhaupt wel elke dag zijn kleren moet wassen. Een slimme auto zet de gebruiker aan tot zuiniger rijgedrag, maar niet tot denken of de auto ook wel een dagje in de garage kan blijven staan. Volgens Morozov zou persuasieve technologie dus moeten stimuleren over welke dingen juist zijn om te doen.

### **Machtsverhoudingen: wie stelt de norm?**

Een gebruiker heeft in relatie met persuasieve technologie niet de mogelijkheid om een discussie aan te gaan met de technologie zoals dat bij een menselijke gesprekspartner wel mogelijk is. Dat zorgt voor een asymmetrische relatie in deze communicatie: de norm wordt in de technologie vastgelegd, en de gebruiker wordt daar eenzijdig aan blootgesteld. Spahn (2012) beargumenteert daarom dat het van belang is dat de gebruiker zoveel mogelijk invloed heeft over hoe deze norm wordt bepaald, en bewust instemt met de inzet van persuasieve technologie. Wanneer een gebruiker zelf besluit een digitale fitnesscoach aan te schaffen kunnen we van deze instemming uitgaan. Wanneer persuasieve technologie echter wordt ingezet in de context van een werkomgeving, of binnen een verzekeringscontext, wordt deze kwestie problematischer (Timmer et al. 2015). Dit roept de vraag op of de werkgever of verzekeraar de normen voor gedragsverandering voor een werknemer of klant mogen bepalen, of dat dit een inbreuk is op zijn autonomie. De Autoriteit Persoonsgegevens deed recentelijk uitspraak over de inzet van wearables

door werkgevers in relatie tot het verzamelen van persoonsgegevens,<sup>32</sup> maar uitspraken over hoe werkgevers wearables mogen inzetten voor gedragssturing ontbreken nog.

## 3.4 Socio-culturele wereld

### 3.4.1 Augmented reality & Virtual reality

Het gebied van augmented reality en virtual reality (VR) is sterk in ontwikkeling. Bij augmented reality (AR) wordt de echte wereld vermengd met virtuele informatie, animaties of objecten. In feite wordt er een extra digitale laag aan informatie toegevoegd aan onze realiteit, bijvoorbeeld via een slimme bril zoals de Google Glass. Bij virtual reality vind de interactie plaats in een volledig virtuele, driedimensionale, interactieve en computer-gegenereerde omgeving waarin gebruikers een kunstmatige ervaring beleven. De lancering in 2012 van de Oculus Rift VR-bril, die zulke mogelijkheden biedt, zorgde toen voor veel aandacht voor virtual reality. Het bedrijf werd in 2014 voor twee miljard dollar gekocht door Facebook dat grootste plannen heeft met virtual reality. 'Na games gaan we van Oculus een platform maken voor allerlei andere ervaringen. Stel je voor dat je aan het veld zit bij een wedstrijd, studeert in een klaslokaal met studenten en leraren van over de hele wereld of een persoonlijk consult hebt met een dokter – gewoon door thuis een bril op te zetten',<sup>33</sup> aldus ceo Mark Zuckerberg. In de toekomst kan virtual reality een belangrijk onderdeel van ons sociale leven worden. De sociale media-mogelijkheden worden hierdoor enorm uitgebreid: mensen kunnen niet alleen momenten online doorbrengen met vrienden, maar er hele ervaringen en avonturen beleven.

#### **Privacy: Little brother (AR) en misbruik van virtuele avatars (VR)**

Een veelbesproken ontwikkeling in augmented reality was de lancering van de Google Glass in 2013, een draagbare computer in de vorm van een bril die informatie projecteert op een klein display voor je ogen. Google stopte begin 2015 met de productie van Google Glass als consumentenproduct om zich voorlopig te richten op zakelijke toepassingen.<sup>34</sup> Een van de redenen waarom de publieke lancering van de Google Glass mislukte was dat er veel publieke onrust ontstond over de mogelijkheid om privégesprekken en sociale interacties (ongevraagd) te filmen met de bril. De ontwikkeling van AR leidt tot zorgen over een zogenaamd Little-Brother-scenario: in plaats van een overheid die iedereen bespied, zijn het burgers en bedrijven die elkaar continu bespieden. Slimme brillen of lenzen zijn ideale middelen om mensen te volgen en te bespieden zonder dat mensen dat in de gaten hebben (Geser 2010). Zeker als zo'n AR-bril of -lens is uitgerust met een app voor gezichtsherkenning krijgt de gebruiker realtime-informatie over de persoon voor hem. Zo'n bril stelt de drager dus in staat van alles te registreren, zonder dat anderen zien dat registratie plaatsvindt. Dat dit volgens de wet niet mag, zal waarschijnlijk kwaadwillenden niet tegenhouden, omdat het haast ondoenlijk is ze te traceren.

Daarnaast leidt de slimme bril of lens nog tot een ander vraagstuk: van wie zijn de beelden die de bril registreert? Met andere woorden: heeft de drager van de slimme bril of lens het exclusieve recht

---

<sup>32</sup> [autoriteitpersoonsgegevens.nl/nl/nieuws/ap-verwerking-gezondheidsgegevens-wearables-door-werkgevers-mag-niet](http://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-verwerking-gezondheidsgegevens-wearables-door-werkgevers-mag-niet)

<sup>33</sup> [nu.nl/internet/3735946/waarom-heeft-facebook-interesse-in-virtual-reality.html](http://nu.nl/internet/3735946/waarom-heeft-facebook-interesse-in-virtual-reality.html)

<sup>34</sup> [theguardian.com/technology/2015/jul/31/google-glass-wearable-computer-businesses](http://theguardian.com/technology/2015/jul/31/google-glass-wearable-computer-businesses)



op zijn/haar eigen waarneming (Brinkman 2014; Wolf, Grodzinsky & Miller 2015)? Google had octrooi aangevraagd en gekregen op de technologie die via het volgen van oogbewegingen het mogelijk maakt dat het bedrijf ziet waar een drager van een Google Glass naar kijkt.<sup>35</sup> Hierdoor kan zo'n bedrijf niet alleen beschikken over het beeld dat de drager van de bril ziet, maar krijgt ook informatie over wanneer en naar wat de drager precies kijkt. Deze data kunnen voor andere bedrijven zeer bruikbaar zijn voor bijvoorbeeld profiling en kunnen daardoor onderdeel worden van het businessmodel van een bedrijf dat de beelden registreert.

In virtual reality gaat het privacyvraagstuk over de nieuwe manieren waarop het gedrag van mensen gevolgd kan worden in virtuele ruimten. Spelfabrikanten zoals Knack<sup>36</sup> laten zien dat aan de manier waarop iemand een spel speelt in de virtuele wereld veel kan worden afgeleid over zijn persoonlijkheid, de manier van samenwerken en hoe iemand problemen oplost (Peck 2013). Zeker wanneer sociale interacties zich meer verplaatsen naar sociale netwerken in VR – wat de ambitie van Facebook is – is de impact op privacy groot. Niet alleen de controle over persoonlijke informatie komt onder druk te staan, ook de mogelijkheid om te bepalen wie wel en niet deel uitmaakt van een interactie is lastiger in een virtuele ruimte. Bovendien kan continue monitoring leiden tot sociaal conformisme, verminderde authenticiteit en zelfcensuur (O'Brolchain 2016). Tot slot is het ook een vraagstuk hoe moet worden omgegaan met beeltenissen van personen. Wanneer in VR realistische avatars gemaakt kunnen worden – bijvoorbeeld van bekende personen – levert dat een vraagstuk op over hoe zij controle houden over hun eigen beeltenis. Hoe kan worden voorkomen dat een avatar in VR voor ongewenste activiteiten wordt ingezet in een nieuwe virtuele vorm van identiteitsmisbruik?

### **Veiligheid: psychische schade in virtuele werelden (VR)**

Het hierboven beschreven misbruik van beeltenissen in virtuele werelden roept de vraag op wat de acties in virtuele wereld betekenen. Duitse filosofen Madary en Metzinger (2016) hebben een eerste poging gedaan tot het opstellen van een gedragscode bij het onderzoeken en gebruiken van virtual reality-technologieën. Ze zijn voornamelijk geïnteresseerd in de risico's van VR-technologieën die gebruikers het gevoel geven zich in een ander lichaam te bevinden dan hun eigen lichaam, en met name in die situaties waarin gebruikers interacteren met andere virtuele of echte mensen. In deze situaties kunnen onethische gedragingen plaatsvinden die reeds in computerspelen tot controverse hebben geleid (Seddon 2012). Een bekend voorbeeld is dat iemand aangifte deed omdat haar avatar zou zijn aangerand in het computerspel *Second Life*. Volgens Madary en Metzinger (2016) is de emotionele betrokkenheid binnen een virtuele omgeving waarin we feitelijk belichaamd zijn (*actually embodied*) vele malen groter. Dat betekent dat de psychische schade die iemand oploopt ten gevolge van een aanranding in virtual reality zeer waarschijnlijk groter zal zijn dan voorgaande gevallen in het spel *Second Life*. De verwachting is dat in de nabije toekomst mensen elkaar vaker gaan opzoeken in virtuele omgevingen en dat sociale netwerken als Facebook deze mogelijkheden ook gaan ondersteunen. Een succesvolle implementatie hangt voor een groot deel af van hoe

---

<sup>35</sup> patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnethtml%2FPTO%2Fsearch-adv.htm&r=36&p=1&f=G&l=50&d=PTXT&S1=%2820130813.PD.+AND+Google.ASNM.%29&OS=ISD/20130813+AND+AN/Google&RS=%28ISD/20130813+AND+AN/Google%29

<sup>36</sup> Knack is een producent van zogenaamde *assessment games*, computerspelletjes die ontworpen zijn om een oordeel te kunnen vormen over iemands prestaties in een werkomgeving.

mensen zich zullen gedragen in virtuele ruimten. Een ethische gedragscode of bepaalde regulering van het gedrag in deze virtuele ruimten is dan ook wenselijk.

Er is nog weinig onderzoek gedaan naar de effecten van de emotionele betrokkenheid in VR en hoe ervaringen in VR doorwerken in de echte wereld (Kizza 2013). De eerste ervaringen met therapievormen die in VR wordt aangeboden – bijvoorbeeld om van een fobie af te komen, of om lastige sociale situaties zoals een sollicitatiegesprek te oefenen – laten wel zien dat VR positieve bijdragen kan leveren aan de behandeling van angsten en stoornissen.<sup>37</sup> Omgekeerd zou daarmee ook kunnen worden verwacht dat ook emotionele schade in de virtuele wereld kan doorwerken in de echte wereld. Madary en Metzinger (2016) pleiten ervoor dat deze zaken eerst goed worden onderzocht, zodat een introductie in de markt van deze VR-technologieën op een ethisch verantwoorde manier plaats zal vinden.

### **Menselijke waardigheid: desocialisatie en vervreemding (VR)**

VR-technologie tarta het gebruikelijke onderscheid tussen virtuele en werkelijke wereld. Dit roept de vrees op dat mensen op een gegeven moment 'echt' niet meer van 'nep' kunnen onderscheiden. Melson et al. (2009) zijn bang dat door het massale gebruik van deze technologieën onze interactie met de natuur zal vervangen. Daardoor zullen we ook de helende en creatieve kracht van de natuur gaan missen. Louv (2005) spreekt van het *nature deficit disorder*. Madary en Metzinger (2016) noemen zelfs het gevaar dat veelvuldige gebruikers van VR de werkelijke wereld en hun lichaam als onwerkelijk beschouwen, en dat hun gevoel van werkelijkheid exclusief verschoven is naar de virtuele omgeving. Dit leidt tot verwaarlozing van hun daadwerkelijke fysieke en sociale omgeving.

Wat betreft het verschuiven van sociale contacten naar de virtuele wereld, is Turkle (2011) bang dat mensen hun sociale competenties – bijvoorbeeld omgaan met afwijzing en herstellen van ruzies – verliezen als we in de toekomst hoofdzakelijk virtuele contacten hebben.<sup>38</sup> De vrees van Turkle voor dit verlies is gebaseerd op haar langdurig onderzoek naar de invloed van sociale media en mobiele telefoons op de communicatie tussen jongeren. Turkle stelt dat de jongste generatie veel minder empathisch is dan haar voorgangers omdat intimiteit vermeden kan worden en daardoor relaties via sociale media of virtual reality minder verplichtend zijn. Dotson (2014) voorziet zelfs een toekomst waarbij we contact hebben met virtuele personen. Dit draagt volgens hem bij aan een ongewenste verschuiving in de collectieve opvatting van 'authentieke socialiteit'. Een kleine groep Japanse mannen – bijgenaamd Otaku – geven al aan dat ze een virtuele vriendin prefereren boven een echte relatie: 'With real girlfriends you have to consider marriage. So I think twice about going out with a 3D woman.' (Rani 2013). Een ander risico is volgens O'Brolcháin et al. (2016) dat VR verslavend kan werken, zoals de virtuele wereld ook andere verslavingen heeft voortgebracht. Gokken en porno zijn door het internet bijvoorbeeld constant beschikbaar en zorgen daardoor voor nieuwe online vormen van verslavingen. Kortom: aandacht voor de invloed van sociale media en virtual reality op onze sociale vaardigheden is niet alleen een kwestie van de lange termijn, maar nu reeds nodig.

---

<sup>37</sup> [mmi.tudelft.nl/vret/index.php/Virtual\\_Reality\\_and\\_Phobias](http://mmi.tudelft.nl/vret/index.php/Virtual_Reality_and_Phobias)

<sup>38</sup> Zie ook Sullins (2012).

### 3.4.2 Digitale platformen

Digitale platformen maken het mogelijk dat transacties slim en efficiënt worden georganiseerd. Uber en Airbnb zijn daar de meest zichtbare voorbeelden van. Er zijn nog tal van andere initiatieven met name met betrekking tot de deeleconomie: 'Het fenomeen dat consumenten elkaar gebruik laten maken van hun onbenutte consumptiegoederen, eventueel tegen betaling' (Meelen & Frenken 2014). Voorbeelden zijn Marktplaats, Peerby ('Leen makkelijk en snel spullen van je burens'),<sup>39</sup> ParkFlyRent ('Parkeer gratis bij het vliegveld en verhuur je auto volledig verzekerd')<sup>40</sup> en Thuisafgehaald ('Maaltijden delen met je burens').<sup>41</sup> Deze digitale platformen kennen vele voordelen, zoals gebruikersgemak, efficiëntie en mogelijk duurzaamheid, aangezien via de deeleconomie producten mogelijk vaker en daarmee efficiënter gebruikt kunnen worden. Daarnaast spelen bij digitale platformen tal van ethisch-maatschappelijke kwesties die serieuze aandacht verdienen.

#### Privacy: inzicht in alle platform interacties

Ook bij digitale platformen speelt de kwestie van privacy. Alle transacties en interacties die binnen het platform plaatsvinden zijn te volgen door de beheerder van het platform, en veel van deze transacties bevatten gevoelige informatie. Platformen kunnen eenvoudig met simpele tools hun gebruikers volgen. Met name de wijze waarop (medewerkers van) Uber met de privacy van zowel haar chauffeurs als klanten omging, heeft veel opzien gebaard (Rogers 2015). Zo werd bekend dat Uber met hun zogenaamde real-time trackingsysteem 'God View' zowel hun klanten als chauffeurs volgden. In een blogpost van een medewerker van Uber, die overigens verwijderd is, werd met veel bravoure gesteld dat Uber op basis van de data die ze verzamelen kan inschatten wie van hun klanten een one-night-stand heeft gehad. Die conclusie kan men trekken wanneer twee verschillende klanten 's avonds worden afgezet op een adres waar ze beiden niet wonen, en 's ochtends worden opgehaald en dan ieder weer op hun eigen adres worden afgezet.<sup>42</sup> Daarnaast bleek dat Uber een datalek niet had gemeld waardoor persoonlijke informatie van vijftig duizend Uber-chauffeurs maandenlang online stond. Nadat een schikking van twintig duizend dollar werd getroffen met justitie in New York heeft Uber haar privacybeleid aangescherpt. 'God View' is inmiddels geanonimiseerd en het aantal medewerkers dat bij persoonlijke informatie van chauffeurs kan is kleiner geworden. Daarnaast zijn de locatiedata van Uber-chauffeurs en klanten versleuteld.<sup>43</sup> Deze data zijn echter wel in te zien met een wachtwoord dat bekend is bij Uber. Scherp toezicht op privacyrichtlijnen voor platformen die een neiging hebben zich te onttrekken aan regelgeving, lijkt hard nodig. Op deze manier kan duidelijk gemaakt worden welke data verzameld worden, hoe ze worden verzameld en gebruikt, en of ze worden doorverkocht (Scholz 2016b).

#### Controle: transparantie van sturende algoritmen

Platformen maken gebruik van algoritmes om tot bepaalde keuzes en beslissingen te komen. Voorheen waren algoritmes deterministisch – van tevoren is door de programmeur voor elke situatie een actie bepaald – en was het mogelijk voor een mens te achterhalen hoe het algoritme tot een beslissing kwam. Door onder ander kunstmatige intelligentie volgen algoritmes geen vooraf

<sup>39</sup> peerby.com/nl

<sup>40</sup> parkflyrent.nl

<sup>41</sup> thuisafgehaald.nl

<sup>42</sup> whosdrivingyou.org/blog/ubers-deleted-rides-of-glory-blog-post

<sup>43</sup> buzzfeed.com/johanabhuiyan/uber-settles-godview#.yvb4dKINR

bepaalde set van regels maar maken ze gebruik van zelflerende statistische technieken. Daardoor zijn de beslissingen die een algoritme maakt voor de mens haast ondoorgrondelijk (Scholz 2016a). Om manipulatie te voorkomen is het daarom van groot belang dat we inzicht hebben in hoe dergelijke algoritmen tot bepaalde keuzes komen. In het onderzoek van psycholoog Robert Epstein bleek hoe zoekresultaten de voorkeuren van kiezers sterk kunnen beïnvloeden door de volgorde van de resultaten in een zoekmachine, zoals Google, te wijzigen. Volgens Epstein vormt dit een ernstige bedreiging voor de democratie.<sup>44</sup> Maar algoritmen worden op veel meer terreinen ingezet. Bij Uber wordt bijvoorbeeld de manier waarop met vraag en aanbod van mobiliteit wordt omgegaan ook door algoritmen besloten. De opkomst van de blockchain schetst een toekomst waarin organisaties in de toekomst volledig geautomatiseerd en gedecentraliseerd in code kunnen worden vastgelegd (Wright & De Filippi 2015). Een organisatie zoals een verzekeraar zou aan de hand van bepaalde in software vastgelegde regels geautomatiseerd geld kunnen innen, en kunnen uitkeren wanneer een klant aan bepaalde voorwaarden voldoet, zonder dat ergens in die beslisprocessen nog een mens aan te pas komt. Met die toenemende automatisering rijst de vraag hoe er controle en toezicht gehouden kan worden op dergelijke systemen.

Transacties tussen Uber en klanten hebben al enkele malen geleid tot misverstanden omdat klanten niet op de hoogte waren van het algoritme dat Uber toepaste. Bij de ontknoping van het gijzelingsdrama in Sydney in december 2014 probeerden veel mensen via een Uber-taxi weg te komen van de plek des onheils. Het Uber-algoritme signaleerde de sterk verhoogde vraag en rekende vervolgens vier keer de normale ritprijs.<sup>45</sup> Op sociale media werd Uber verweten dat ze misbruik maakte van de gijzelings situatie. In een blogpost verontschuldigde Uber zich: 'Surge pricing is algorithmic and kicks in automatically when demand for rides outstrips the supply of cars that are on the road.' Wanneer algoritmes geen rekening houden met onvoorziene situaties kan dat dus tot onwenselijke gevolgen leiden.

## Rechtvaardigheid: uitbuiting en uitsluiting

Platformen zorgen ervoor dat de gebruiker een dubbele rol heeft; als producent en als consument. Met spreekt in dit geval van *prosumers*. De kracht van platformen is dat ze vraag en aanbod op een efficiënte manier bij elkaar brengen en via slimme beoordelingsmechanismen het vertrouwen scheppen dat transacties – zoals het verhuren van een appartement aan een onbekende – mogelijk maakt. Om efficiënt in te kunnen springen op een veranderende vraag werken platformen veelal met een flexibele schil van aanbieders die op afroep beschikbaar zijn. Om deze reden wordt ook wel gesproken over de *on-demand economy*. Het feit dat aanbieders op afroep hun diensten aanbieden en niet in een vast dienstverband worden aangenomen kan traditionele mechanismen van werknemersbescherming onder druk zetten, waardoor uitbuiting op de loer ligt. Zo zouden chauffeurs van Uber te lange werkdagen maken en weinig in te brengen te hebben als het bedrijf besluit de tarieven voor ritten aan te passen (Rogers 2015).

Daarnaast kunnen platformen eenzijdig besluiten een gebruiker de toegang te ontfemen tot het platform. Voor gebruikers die voor hun inkomsten afhankelijk zijn van toegang tot het platform kan

---

<sup>44</sup> [politico.com/magazine/story/2015/08/how-google-could-rig-the-2016-election-121548](http://politico.com/magazine/story/2015/08/how-google-could-rig-the-2016-election-121548)

<sup>45</sup> [thestar.com/news/world/2014/12/15/uber\\_backtracks\\_on\\_price\\_hikes\\_during\\_sydney\\_drama](http://thestar.com/news/world/2014/12/15/uber_backtracks_on_price_hikes_during_sydney_drama)

dit verstrekken gevolgen hebben. Huidige casuïstiek laat bovendien zien dat platformen makkelijk over gaan tot het uitsluiten van bepaalde gebruikers. Voor Uber-chauffeurs mag hun beoordeling niet onder de 4.6 sterren komen (4.8 sterren is het gemiddelde). Gebeurt dat wel, dan kunnen zij worden verwijderd van de dienst. Rogers (2015) beschrijft dat het continue systeem van reviews ervoor zorgt dat aanbieders zich altijd vriendelijk en vrolijk moeten gedragen. Naast hun fysieke arbeid wordt van hen verwacht een bepaalde 'emotionele arbeid' te verrichten. Waar reguliere taxichauffeurs de vrijheid hebben om chagrijnig achter het stuur te zitten, kan dat voor Uberchauffeurs betekenen dat ze hun bron van inkomsten kwijtraken.

### **Machtsverhoudingen: oneerlijke concurrentie en monopolisering**

Volgens Scholz (2016b) is het succes van bepaalde platformen niet alleen te wijten aan de technologische mogelijkheden, maar hangt er ook mee samen dat de betreffende bedrijven 'illegaliteit als methode' hanteren. Dit leidt tot oneerlijke concurrentie tussen platformen en reguliere bedrijven, omdat platformen zich niet (hoeven te) houden aan regels of vergunningen die gelden voor reguliere bedrijven. Airbnb maakt het mogelijk dat particulieren zonder vergunning kamers verhuren en dat niet aan de veiligheidseisen en belastingplicht wordt voldaan waar reguliere hotels zich wel aan moeten houden. En UberPop-chauffeurs hoeven zich niet aan de rij- en rusttijden te houden, hoeven niet aan de veiligheidsvoorschriften te voldoen waar taxi's aan moeten voldoen, en hoeven geen btw in rekening te brengen. Daarnaast verdient de gemiddelde UberPop-chauffeur minder dan het minimumloon en zien de meeste chauffeurs dit als een bijbaantje.<sup>46</sup> UberPop werd in december 2014 in Nederland verboden, maar Uber bleef de dienst nog bijna een jaar aanbieden, en betaalde zelfs de boetes van illegaal rijdende UberPop-chauffeurs.<sup>47</sup> In november 2015 is Uber uiteindelijk gestopt met het aanbieden van de taxidienst UberPop, omdat volgens het bedrijf 'de dienst een belemmering vormt voor een constructieve dialoog over modernisering van bestaande wet- en regelgeving.'<sup>48</sup>

Volgens Frenken et al. (2015) is het logisch dat er aanvankelijk een gedoogbeleid is om experimenten de ruimte te geven en de effecten te kunnen inschatten. Toch pleiten de auteurs voor een heldere regelgeving als platformen zoals Airbnb en Uber zo snel groeien dat ze ontwrichtende en onverwachte effecten op bestaande sectoren en voor de samenleving als geheel hebben. Hierbij kunnen we denken aan machtsconcentraties van dergelijke platformen, met monopolies met hoge winstmarges als gevolg. Deze monopolies kunnen bestaan doordat dergelijke platformen gekenmerkt worden door netwerkeffecten zoals we dat hebben gezien bij internetbedrijven als Google (in zoeken op internet), Facebook (in sociaal netwerken) en WhatsApp (in mobiele berichten). WhatsApp bijvoorbeeld werkt alleen als er een groot netwerk van gebruikers op zit. Als zo'n app dan eenmaal de grootste is, is het haast onmogelijk om hiermee te concurreren, omdat er sprake is van *the winner takes all* (Kreijveld 2014). Kreijveld stelt dat platformen hun bereik ook relatief eenvoudig kunnen vergroten door nieuwe diensten te integreren en toe te voegen (zoals Uber, dat zich nu ook bezighoudt met pakketbezorging<sup>49</sup>) waardoor de vraag rijst of platformen daarmee niet te groot worden. Een gevolg is dat gebruikers afhankelijk worden van zo'n platform,

<sup>46</sup> [volkskrant.nl/economie/uberpop-chauffeur-haalt-vaak-minimumloon-niet-a3823583](http://volkskrant.nl/economie/uberpop-chauffeur-haalt-vaak-minimumloon-niet-a3823583)

<sup>47</sup> [nos.nl/artikel/709243-uber-betaalt-desnoods-boetes](http://nos.nl/artikel/709243-uber-betaalt-desnoods-boetes)

<sup>48</sup> [nrc.nl/nieuws/2015/11/18/uber-stopt-met-uberpop-in-nederland](http://nrc.nl/nieuws/2015/11/18/uber-stopt-met-uberpop-in-nederland)

<sup>49</sup> [rush.uber.com/how-it-works](http://rush.uber.com/how-it-works)

omdat het heel lastig is om van een ander platform gebruik te maken waar het netwerk te klein is om interessant te zijn. Ook opgebouwde data en connecties binnen een platform en andere diensten die gekoppeld zijn aan het opgebouwde profiel maken het voor een gebruiker moeilijk om naar een andere dienst over te stappen; een zogenoemd *lock-in*-effect.

### 3.5 Digitale wereld

Zoals we in hoofdstuk 2 hebben besproken leidt de digitalisering van de materiële, biologische en socio-culturele wereld tot een steeds verder uitdijende digitale datawereld. In de digitale wereld worden gegevens verwerkt en geanalyseerd, en op basis daarvan worden zowel door mensen als door geautomatiseerde systemen beslissingen genomen die vervolgens weer effect hebben in de fysieke wereld. Ontwikkelingen op het gebied van big data, slimme algoritmen en artificiële intelligentie (AI) zijn dan ook een onmisbaar onderdeel van de hiervoor besproken technologieën. Zo zijn spelen die ontwikkelingen een rol bij Internet-of-Things-apparaten die informatie versturen naar de cloud (big data) en tegelijkertijd door data en algoritmen uit de cloud worden aangestuurd om een bepaalde actie uit te voeren in de fysieke wereld. Omdat de vraagstukken omtrent big data, algoritmen en AI in elkaar overlopen, bespreken we deze ontwikkelingen hier samen als onderdeel van de digitale wereld.

#### Privacy: het reguleren van big data

Er is door digitalisering een levendige handel in informatie ontstaan. 'Big data' wordt soms ook wel 'het nieuwe goud' genoemd. De waarde van data is veelal dat ze het mogelijk maakt om betere beslissingen te nemen, bijvoorbeeld over welke consument welke advertentie te zien moet krijgen, of over welke personen onderzocht moeten worden als mogelijke fraudeurs. Het vraagstuk van privacy is hiervoor al meermaals besproken. De specifieke uitdaging die big data met zich meebrengen op het gebied van privacy zijn het hergebruik en de mogelijke combinaties van verschillende gegevensbronnen. Daarbij is een belangrijk kenmerk van big data dat het van tevoren niet duidelijk is welke inzichten er uit data gehaald kunnen worden. Zo lieten onderzoekers zien dat op basis van Facebook-likes voorspellingen konden worden gedaan over onder andere iemands seksuele voorkeur, religieuze en politieke oriëntaties, persoonlijke karaktereigenschappen en gebruik van verslavende middelen (Kosinsky et al. 2012). Overheden kijken ook naar de mogelijkheden van big data. Een voorbeeld is het Systeem Risico Indicatie (SyRI) waarin data over onder andere boetes, schulden, uitkeringen, onderwijs en inburgering binnen een beveiligde digitale omgeving versleuteld, gecombineerd en geanalyseerd worden om effectiever te zoeken naar mensen die uitkeringen of toeslagen misbruiken. Het SyRI systeem werd door zowel de Autoriteit Persoonsgegevens en de Raad van State bekritiseerd vanwege de impact op de privacy (WRR 2016). Naar aanleiding van deze kritiek is het systeem op een aantal punten aangepast, maar niet alle aanbevelingen werden overgenomen.

Het combineren en hergebruik van big data lijkt haaks te staan op het doelbindingsprincipe dat een van de pijlers is van de wetgeving op het gebied van gegevensbescherming (Kool et al. 2015). Verschillende auteurs pleitten er dan ook voor dat wetgeving en toezicht zich in het tijdperk van big data meer zouden moeten richten op verantwoordelijkheden van bedrijven (accountability) en hoe data gebruikt wordt (Podesta et al. 2014; Cate et al. 2014). Maar zijn er ook tegengeluiden die pleiten dat doelbinding een belangrijk mechanisme is om ongebreidelde verzameling en *data-*

*obesitas* tegen te gaan (Hildebrandt 2015). Op Europees niveau wordt met een wijziging van de dataproctiewetgeving getracht om de vragen van big data problemen het hoofd te bieden. De nieuwe Europese Dataproctieverordening (EU 2016/679) bouwt voort op de principes van de dataproctierichtlijn (95/46/EC), voegt daar een aantal nieuwe plichten en verantwoordelijkheden voor dataverwerkers aan toe, en versterkt de rechten van het individu. Uit de verordening blijkt dat het onderwerp data hoog op de agenda staat. Tegelijkertijd is er ook discussie over de vraag of de wettelijke aanpassingen adequaat zijn om de uitdagingen die digitalisering met zich meebrengt aan te pakken. Met name waar het gaat om profilering biedt het juridische kader slechts ten dele bescherming (Kool et al. 2015).

### **Autonomie: filteren en vrijheid van meningsuiting**

Waar het verzamelen van data overgaat in de volgende fase van de cybernetische loop, in het analyseren en toepassen, worden nieuwe vragen opgeroepen. Online platformen spelen een steeds grotere rol bij het bepalen van welke informatie en welk nieuws mensen zien. Een bekend voorbeeld is hoe Google-zoekresultaten van verschillende personen variëren door een personalisatie-algoritme dat onder andere kijkt naar eerdere zoekopdrachten (Pariser 2011). Dat roept vragen op met betrekking de sturende rol van grote platformen en ook over de vrijheid van meningsuiting. Een recent voorbeeld is de verwijdering van de iconische World Press Photo uit 1972 waarop een meisje staat afgebeeld dat slachtoffer is van een napalmaanval (het 'Napalmmeisje' zoals de foto is gaan heten) door Facebook. Facebook kreeg veel kritiek te verduren en maakte later de verwijdering ongedaan.<sup>50</sup> Ook andere platformen zoals Google en Twitter (en ook Facebook), zijn bekritiseerd omdat ze de verspreiding van 'nepnieuws' zouden faciliteren.<sup>51</sup> Dat leidt tot een discussie over de rol en verantwoordelijkheden van platformen in relatie tot de vrijheidsmeninguiting en het filteren van informatie. Deze discussie deed in de nasleep van de Amerikaanse presidentiële verkiezingen in 2016 veel stof opwaaien. De platformen onderzoeken welke actie ze kunnen nemen tegen nepnieuws.<sup>52</sup>

### **Controle: inzicht in algoritmen en AI**

Bij het analyseren en het nemen van beslissingen op basis van gegevens, spelen software en geautomatiseerde systemen een steeds grotere rol. De verwachting is dat deze trend door zal zetten. Algoritmes spelen reeds een rol bij het bepalen van persoonlijke online informatievoorziening op sociale netwerken, het bepalen van kredietwaardigheid, het opsporen van fraudeurs en terrorismeverdachten, en het handelen op de beurs (Pasquale 2015). IBM voert experimenten uit met het inzetten van de supercomputer Watson om artsen te ondersteunen bij het doen van medische diagnostiek. En ook binnen de rechtspraak wordt gekeken hoe geautomatiseerde systemen kunnen helpen bij het analyseren van bergen aan juridische casuïstiek en het voorzien van advies.<sup>53</sup>

---

<sup>50</sup> <http://www.volkskrant.nl/buitenland/facebook-maakt-verwijdering-napalmmeisje-na-kritiek-ongedaan--a4373624/>

<sup>51</sup> <http://www.rtlnieuws.nl/technieuws/nepnieuws-verspreid-door-aanpassing-zoekalgoritme-google>, <http://www.reuters.com/article/us-twitter-facebook-commentary-idUSKBN13W1WO>

<sup>52</sup> [http://www.nytimes.com/2016/11/15/technology/google-will-ban-websites-that-host-fake-news-from-using-its-ad-service.html?\\_r=1](http://www.nytimes.com/2016/11/15/technology/google-will-ban-websites-that-host-fake-news-from-using-its-ad-service.html?_r=1)

<sup>53</sup> [theatlantic.com/sponsored/ibm-transformation-of-business/watson-takes-the-stand/283](http://theatlantic.com/sponsored/ibm-transformation-of-business/watson-takes-the-stand/283)

De afgelopen jaren is de discussie over controle op de onderliggende algoritmen in geautomatiseerde systemen vanuit verschillende hoeken aangekaart (Zarsky 2013, Pasquale 2015, Kool et al. 2015, WRR 2016). De Duitse regering bracht onlangs een position paper uit waarin ze stelt dat online platformen – zoals Google en Facebook – inzicht moeten geven in hoe hun algoritmen werken, bijvoorbeeld in het voorsorteren van nieuws of zoekresultaten.<sup>54</sup> Aangezien de complexiteit van de algoritmen en de snelheid waarmee computers beslissingen maken zeer groot zijn, is het moeilijk om inzicht in te krijgen hoe een bepaald besluit tot stand is gekomen, en dergelijke besluiten op fouten te controleren en waar nodig te corrigeren. Met het oog op de toepassing van geautomatiseerde analysesystemen in de rechtspraak of de medische wereld is dergelijke controle onontbeerlijk. Hoe wordt er verantwoordelijkheid afgelegd over het besluit dat een computer neemt? Kan bijvoorbeeld het advies wat een rechter of aanklager krijgt afhangen van de leverancier waarbij de software is aangeschaft? Om inzicht en controle mogelijk te maken werkt IBM voor Watson aan een systeem dat Watson Paths heet. Hiermee moet het mogelijk worden dat de computer kan toelichten hoe bijvoorbeeld een bepaalde beslissing op medisch gebied tot stand is gekomen.<sup>55</sup>

Diakopoulos (2016) heeft een eerste poging gedaan om een transparantie-standaard voor het gebruik van algoritmes te ontwikkelen, om zo controle en toezicht op algoritmes mogelijk te maken. Hij beschrijft hierin vijf categorieën waarmee rekening moet worden gehouden om transparantie te waarborgen:

1. Menselijke betrokkenheid. Helder moet zijn wie (van het bedrijf) controle heeft over het algoritme; wie verantwoordelijk is; en wie de ontwikkelaars zijn van het algoritme.
2. Data. Helderheid over de kwaliteit, nauwkeurigheid, onzekerheid en volledigheid van de data, en welke data gebruikt worden en welke data gecombineerd worden.
3. Het model. Helder moet zijn hoe data gecombineerd worden, hoe bepaalde data gewogen worden en welke aannames er gemaakt worden.
4. Inferentie. Wat is de foutmarge? Bijvoorbeeld: hoeveel 'false positives' en 'false negatives' zijn er, en zijn die fouten te wijten aan data-input, menselijke betrokkenheid of het algoritme?
5. Gebruik van het algoritme. Helder moet zijn op welk moment en in welke gevallen een algoritme wordt ingezet.

Het probleem hierbij is echter dat bedrijven zullen claimen dat ze niet precies kunnen aangeven hoe hun algoritme werkt, omdat dit een onderdeel vormt van hun strategie. Door het prijsgeven van de werking van hun algoritme kunnen concurrenten eenvoudig het algoritme overnemen en de bijbehorende diensten aanbieden (Gillespie 2014).

Ontwikkelingen in het veld van artificiële intelligentie (AI) maken het vraagstuk van controle en inzicht complexer. Bij zelflerende vormen van AI-systemen kan van tevoren niet worden bepaald hoe ze op bepaalde situaties zullen reageren. Technieken zoals Deep Learning (Zie kader 2.5 in hoofdstuk 2), waarin verschillende lagen van neurale netwerken worden gebruikt, maken het moeilijk om transparantie te bieden en uit te leggen waarom een systeem een bepaalde beslissing neemt. Dat leidt tot zorgen over hoe controle en verantwoording moet worden afgelegd bij de inzet

---

<sup>54</sup> [bmwi.de/DE/Presse/pressemitteilungen,did=764540](http://bmwi.de/DE/Presse/pressemitteilungen,did=764540)

<sup>55</sup> [research.ibm.com/cognitive-computing/watson/watsonpaths.shtml#bid=T7yOxG\\_VXYP](http://research.ibm.com/cognitive-computing/watson/watsonpaths.shtml#bid=T7yOxG_VXYP)



van AI-systemen (Royakkers & Van Est 2015; Helbing et al. 2015). Op de langere termijn zijn er ook zorgen over hoe een zich steeds verder doorontwikkellende AI nog gecontroleerd kan worden door mensen. Zo waarschuwden onder andere internetondernemer Musk en wetenschapper Hawking voor de existentiële dreiging van superintelligente AI (Gibbs 2014; Hawking et al. 2014). Maar ook minder geraffineerde vormen van automatische systemen kunnen voor onvoorziene en lastig te controleren problemen zorgen, in het bijzonder wanneer diverse systemen op een complexe wijze interacteren. Een bekend voorbeeld is de zogenaamde Flash Crash die plaats vond op 6 mei 2010. Door een onvoorzien samenspel van factoren begonnen verschillende geautomatiseerde handelssystemen (die worden ingezet in *high frequency trading*) in enkele seconden grote hoeveelheden aandelen te verkopen waardoor de beurs in enkele minuten miljarden aan waarde verloor om vervolgens de volgende minuten weer grotendeels te herstellen.

### **Rechtvaardigheid: discriminatie en onterechte uitsluiting**

Beoordelingen en geautomatiseerde beslissingen van computers zijn niet feilloos. Fouten in gegevens of verkeerde aannames in een analysemodel kunnen leiden tot een verkeerd oordeel. Dat kan leiden tot ongewenste vormen van discriminatie en uitsluiting door het computersysteem. Het hiervoor beschreven gebrek aan inzicht en transparantie van beslissystemen, maken het moeilijk om in te schatten wanneer een systeem ernaast zit. Voor het individu is het daardoor vaak lastig om tegen het systeem bezwaar aan te tekenen. Dit wordt geïllustreerd door de praktijk van geautomatiseerde kredietwaardigheidsbeoordeling in de Verenigde Staten (Citron & Pasquale 2014). Om te bepalen of iemand geschikt is voor een lening maken veel geldverstrekkers gebruik van geautomatiseerde systemen die op basis van gegevens uit verschillende bronnen een kredietscore berekenen. De gegevens die hiervoor worden gebruikt, en de manier waarop ze worden geanalyseerd zijn voor het publiek niet inzichtelijk; transparantie zou namelijk het bedrijfsgeheim van de beoordelaar kunnen schaden. Hoewel de scores een significante foutmarge hebben, wordt de analyse van de computer vaak blindelings opgevolgd. Omdat de logica achter een bepaalde beslissing niet inzichtelijk is voor klanten is het moeilijk om bezwaar te maken en aan te tonen waar het systeem fout zit (Citron & Pasquale 2014).

Geautomatiseerde systemen brengen een risico op verkeerde oordelen met zich mee. In verschillende studies wordt gewaarschuwd voor onterechte uitsluiting en discriminatie door geautomatiseerde systemen (Zarsky 2013, Podesta et al. 2014, Citron & Pasquale 2014). Door middel van profilering worden mensen in bepaalde categorieën ingedeeld die elk een andere behandeling krijgen. Vanuit het oogpunt van service kan dit voor maatwerk en gemak zorgen. Maar wanneer bepaalde (groepen) mensen hierdoor structureel worden benadeeld is dat problematisch. Zo bleek dat vrouwen die zochten op banen minder vaak advertenties voor hoge functies te zien kregen dan mannen met een gelijk profiel (Datta 2015). Zelfs wanneer geen gebruik wordt gemaakt van gegevens over ras of geloof kan er middels andere variabelen die hier sterk mee correleren toch discriminatie plaatsvinden (Hildebrand 2016:202).

Het profiel dat aan iemand kleeft vanwege zijn gedragshistorie kan zijn opties voor de toekomst beïnvloeden. Dat kan leiden tot een self-fulfilling prophecy: iemand met een goede kredietscore krijgt makkelijk een lening en kan makkelijker aan zijn financiële toekomst werken, terwijl iemand die een hoger risico vormt en aan striktere voorwaarden moet voldoen daardoor ook mogelijk eerder in de problemen komen met terugbetalingen (Citron & Pasquale 2014). De Autoriteit

Persoonsgegevens waarschuwt voor 'digitale predestinatie',<sup>56</sup> het gevaar dat mensen niet meer kunnen 'ontsnappen' aan het digitale profiel dat over hen is opgesteld. Wanneer methoden van profilering en risico-inschatting ook worden ingezet in het veiligheidsdomein, bijvoorbeeld om mogelijke fraudeurs of criminelen op te sporen, komt ook het vermoeden van onschuld onder druk te staan (WRR 2016). Waar normaal pas na een verdenking gegevens over mensen worden verzameld, creëert big data de mogelijkheid dat er al gegevens en risicoprofielen worden opgesteld voordat er een daadwerkelijke verdenking is. De verre gaande mogelijkheden die in het veiligheidsdomein door big data en voorspellende algoritmen worden gecreëerd moeten volgens de WRR (2016) daarom samen gaan met extra toezicht en bescherming van fundamentele rechten.

### **Machtsverhoudingen: verhoudingen private en publieke partijen**

Big data, slimme algoritmen en AI zorgen voor verschuivingen in machtsverhoudingen in de relatie tussen bedrijven, overheden en burgers. De 'publieke ruimte' op het internet – bestaande uit bijvoorbeeld sociale netwerken – is veelal in private handen. Alle interacties die in die pseudo-publieke ruimte plaatsvinden, zijn daardoor eigendom van de platformen, en de informatie die daaruit gegenereerd wordt, kan naar wens worden gebruikt of doorverkocht. En de voorwaarden waaronder interacties plaatsvinden, en welke uitingen wel of niet gewenst zijn, kunnen naar believen door de platformbeheerder worden gewijzigd. Zo is er veel ophef geweest over beslissingen van Facebook om bepaalde uitingen op het platform te verwijderen. Critici stellen dat de huidige situatie leidt tot een vorm van digitaal feudalisme (Meinrath et al. 2011, Balkan 2013, Zuboff 2015, Helbing et al. 2015); een situatie waarin de persoon het eigenaarschap over zichzelf – zijn digitale representatie – kwijt is.

Overheden verzamelen ook steeds meer gegevens over burgers. Helbing et al. (2015) beschrijven een toekomstscenario van *big nudging*, waarbij overheden met behulp van data het gedrag van burgers proberen bij te sturen. Het meest in het oog springende voorbeeld hiervan komt van de Chinese overheid, die van alle burgers een *citizen score* bijhoudt, die een rol speelt bij het bepalen of iemand in aanmerking komt voor bijvoorbeeld een lening, een visum of baan. De dataverzameling door overheden zorgt voor een groeiende informatie-asymmetrie tussen de burger en de overheid, waarbij de burger steeds transparanter wordt en de overheid voor de burger ondoorzichtiger wordt.

In de relatie tussen overheden en bedrijven schuren bedrijven meer tegen publieke taken aan. In dit licht is de rechtszaak interessant waarin Apple werd opgedragen om de FBI te helpen bij het kraken van een iPhone van Syed Rizwan Farook, één van de schutters bij de schietpartij in San Bernardino in december 2015 waarbij 14 doden en 22 zwaargewonden vielen. De FBI wilde met brute kracht de telefoon uitlezen door heel snel achter elkaar alle mogelijke combinaties van cijfers en letters in te voeren op de telefoon. Een iPhone wist zichzelf echter wanneer er tien keer een verkeerde toegangscode wordt ingevoerd. Apple werd opgedragen mee te helpen software te ontwikkelen die dit kon omzeilen. Volgens Apple zal dit een gevaarlijk precedent scheppen, want wanneer deze software in verkeerde handen komt, kan diegene iedere Phone uitlezen. Apple vreesde dat op den

---

<sup>56</sup> [autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-meer-privacywaarborgen-noodzakelijk-bij-toepassingen-big-data](https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-meer-privacywaarborgen-noodzakelijk-bij-toepassingen-big-data)

duur de eis van de FBI ‘would undermine the very freedoms and liberty our government is meant to protect.’<sup>57</sup>

Uiteindelijk wist de FBI samen met een hacker de iPhone van de San Bernardino-schutter zonder de hulp van Apple te kraken. Desondanks toont het voorbeeld dat grote bedrijven, zoals Apple, een sterke machtspositie hebben en een sterke vinger in de pap hebben in hoe hun infrastructuur gebruikt mag worden.

## 3.6 Conclusie

Hierboven beschreven we welke maatschappelijke en ethische vragen er door de digitalisering van de samenleving worden opgeroepen. Daarbij beperkten we ons tot kwesties die samenhangen met ontwikkelingen binnen de in het vorige hoofdstuk geselecteerde technologiegebieden: robotica, Internet of Things, biometrie, persuasieve technologie, platformen, augmented en virtual reality, big data, algoritmen en AI. In deze slotparagraaf vatten we samen welke maatschappelijke en ethische vraagstukken naar voren zijn gekomen en bespreken we welke trends en ontwikkelingen daarin zichtbaar zijn. Dat doen we aan de hand van de zeven overkoepelende thema’s die we aan het begin van dit hoofdstuk hebben onderscheiden. Om het belang van deze ethische en maatschappelijke issues te onderstrepen bespreken we kort de samenhang met belangrijke waarden die vastgelegd zijn in internationale verdragen en grondrechten. Daarnaast laten we zien hoe de maatschappelijke en ethische thema’s samenhangen met een sterke toename in het verzamelen van data, het analyseren van data en het toepassen daarvan, of met andere woorden, een toename van activiteit in elk van de drie fasen van de cybernetische loop die we in hoofdstuk 2 introduceerden.

### 3.6.1 Overzicht van maatschappelijke en ethische vraagstukken

Tabel 3.2 (volgende pagina) geeft per overkoepelend thema een overzicht van de maatschappelijke en ethische vraagstukken die worden opgeroepen door diverse technologische ontwikkelingen op het gebied van digitalisering. In deze subparagraaf lichten we dit overzicht kort toe.

#### *Privacy*

Privacy is het issue dat het meest prominent naar voren komt. Uit de bespreking wordt duidelijk dat privacy over meer gaat dan alleen gegevensbescherming. We zien dat er door *pervasive* en alomtegenwoordige monitoring – door slimme apparaten, robotica en biometrische identificatie – en technieken zoals profilering, nieuwe vraagstukken opkomen rond privacy. Het huidige regime waarbij de gebruiker verantwoordelijk is om via toestemming zijn datastromen te controleren, lijkt niet adequaat voor een toekomst waarin het individu is omgeven door tientallen slimme Internet-of-Things-apparaten met hun eigen datastromen. Daar komt bij dat de reikwijdte van de digitalisering groter wordt. Biometrische technologie zorgt ervoor dat er allerlei informatie, soms zelf van een afstand, van het gezicht en het lichaam afgelezen kan worden, met of zonder toestemming van het individu. Het aflezen van mentale gemoedstoestand uit micro-expressies op het gezicht kan een

---

<sup>57</sup> [apple.com/customer-letter](http://apple.com/customer-letter)

bedreiging vormen voor mentale privacy; het vermogen om onze gedachten en gevoelens privé te houden.

**Tabel 3.2** Maatschappelijke en ethische vraagstukken bij digitalisering

Thema	Vraagstukken
Privacy	Gegevensbescherming, privacy, digitaal huisrecht, mentale privacy, surveillance, doelverschuiving
Autonomie	Keuzevrijheid, vrijheid van meningsuiting, manipulatie, paternalisme
Veiligheid	Informatieveiligheid, identiteitsfraude, fysieke veiligheid
Controle over technologie	Controle en inzicht in algoritmen, verantwoordelijkheid, onvoorspelbaarheid
Menselijke waardigheid	Dehumanisatie, instrumentalisering, <i>deskilling</i> (afleren van vaardigheden), desocialisatie, technologische werkeloosheid
Rechtvaardigheid	Discriminatie, uitsluiting, gelijke behandeling, stigmatisering
Machtsverhoudingen	Onerlijke concurrentie, uitbuiting, relatie burger-overheid-bedrijf

Rathenau Instituut

### *Autonomie*

Autonomie is sterk gerelateerd aan privacy als voorwaarde voor een ongehinderde ontwikkeling van de eigen identiteit. Juist de opkomende uitdagingen op het gebied van privacy – zoals continue monitoring door Internet-of-Things-apparaten – schuren tegen autonomie aan. In hoeverre kan een kind zich nog ongehinderd ontwikkelen als het weet dat de slimme Barbie zijn speelgedrag registreert? Het vraagstuk van autonomie neemt een belangrijker plaats in naarmate technologie meer beslissingen voor mensen voorsorteert, invult of overneemt. Juist die ontwikkeling is duidelijk zichtbaar in allerlei domeinen: online platformen die informatie voorsorteren, slimme omgevingen die op gedrag anticiperen, persuasieve technologie die op bewust en laagbewust niveau invloed kan uitoefenen en robotica die taken deels of volledig overneemt. Het vraagstuk van autonomie waarbij menselijke beslissingsruimte en keuzevrijheid nog bestaat, lijkt daarmee een steeds belangrijker thema te worden.

### *Veiligheid*

Digitalisering biedt mogelijkheden om systemen veiliger in te richten, bijvoorbeeld door data lokaal op te slaan of door versleuteling waardoor alleen informatie die strikt nodig is beschikbaar is. Tegelijkertijd introduceert digitalisering ook nieuwe kwetsbaarheden. Informatieveiligheid en cybersecurity zijn al jaren een belangrijk thema in de digitalisering, maar de huidige ontwikkelingen laten zien dat cyberveiligheid – doordat steeds meer apparaten en diensten aan het internet worden verbonden – een veel grotere fysieke dimensie krijgt. De impact ontstijgt daarmee het niveau van datalekken en misbruik van gegevens, en verschuift naar een nieuw niveau van gehackte auto's waarvan de besturing overgenomen kan worden en pacemakers die tot fatale schokken kunnen worden aangezet. Voor onze fysieke veiligheid wordt het daarom steeds belangrijker dat de veiligheid en het functioneren van digitale systemen goed gewaarborgd wordt.

### *Controle over technologie*

Naarmate er meer processen aan computersystemen worden uitbesteed, wordt de vraag belangrijker hoe menselijke controle over dergelijke systemen kan worden ingericht. Het gaat immers om systemen die medische diagnoses stellen, adviseren en ondersteunen in de rechtspraak, of bij autonome wapentechnologie zelfs beslissingen nemen over leven of dood. Inzicht in de manier waarop deze systemen tot een bepaalde beslissing komen is cruciaal om deze besluiten te kunnen verantwoorden, en om fouten te signaleren en tegen te gaan, bijvoorbeeld wanneer een systeem een onjuiste medische diagnose stelt door een fout in de software of de data. Het samenspel van het toenemend aantal handelende systemen zorgt voor een nieuwe laag van complexiteit, en mogelijke onvoorziene effecten: dat geldt voor de individuele burger waarbij het slimme huis vastloopt door de interacties tussen verschillende ‘slimme’ apparaten, maar ook op maatschappelijk niveau wanneer de beurs crasht door autonoom handelende algoritmen.

### *Menselijke waardigheid*

Op het vlak van menselijke waardigheid zien we dat digitalisering en automatisering – in de vorm van robotica – een rol kunnen spelen in het ontlasten van de mens van ‘onmenselijk’ werk. Tegelijk zijn er ook zorgen dat AI en robotica steeds meer werk kunnen en zullen overnemen van mensen en dat dat zal leiden tot werkeloosheid. Maar er zijn ook subtielere effecten als gevolg van het overnemen van taken door technologie: het afnemen van morele vaardigheden (deskilling) als persuasieve systemen ons richting moreel juist gedrag sturen, of desocialisatie doordat mensen virtuele interacties prikkelender en prettiger vinden dan lastige sociale interacties in de fysieke wereld.

### *Rechtvaardigheid*

Digitalisering zorgt ervoor dat mensen en hun gedrag op allerlei manieren worden geanalyseerd. Daarbij is ook de computer geen onbevooroordeelde beoordelaar, aangezien deze altijd door mensen geprogrammeerd is vanuit bepaalde doelen, veronderstellingen en ideeën. Met het toenemende aantal analyses groeien ook de zorgen over discriminatie, gelijke behandeling en onterechte uitsluiting van mensen. Mensen kunnen op basis van hun profiel toegang tot een lening worden ontzegd, een hogere prijs moeten betalen voor hetzelfde product, of worden aangemerkt als verdachte. Fouten in analyses en profilering kunnen grote consequenties voor individuen hebben en dat is niet wenselijk. Het is tevens zeer onwenselijk dat door profilering systematisch bepaalde groepen mensen worden benadeeld. Een bijkomend probleem is dat er bij geautomatiseerde analyses weinig inzicht is op hoe die analyses tot stand zijn gekomen. Ook in het geval van een foutief oordeel is het moeilijk voor een individu om zo’n fout in een systeem recht te zetten. Kafkaëske scenario’s liggen daarbij op de loer.

### *Machtsverhoudingen*

Machtsverhoudingen zijn in de digitalisering een belangrijk maatschappelijk vraagstuk. Tussen consumenten en bedrijven verandert de relatie doordat producten meer als een dienst worden aangeboden in het Internet of Things. Daarin is zichtbaar dat software een steeds belangrijkere rol speelt in dagelijkse producten en diensten. Degene met de zeggenschap over die software kan in de programmatuur bepalen hoe ze wel of niet gebruikt kan worden, ‘Code is Law’, noemt de Amerikaanse rechtenprofessor Lessig (2006) dat. De machtspositie van een aantal belangrijke internetbedrijven zorgt ook voor discussies over de afhankelijkheid en de positie als

toegangsbeheerder – tot informatie of diensten – die deze bedrijven verwerven. Maar digitalisering verandert ook de relatie tussen burger en overheid, zoals we zien in overheidssystemen waarmee de overheid meer op burgers probeert te anticiperen, zoals door middel van preventief politiewerk (*predictive policing*) of het hierboven genoemde SyRI-systeem. De machtsverhouding verschuift doordat de burger transparanter wordt terwijl de overheid juist ondoorzichtiger wordt.

### 3.6.2 Verzamelen én analyseren én toepassen

De discussie omtrent digitalisering richt zich sinds de jaren zeventig voornamelijk op maatschappelijke en ethische vraagstukken die samenhangen met het op grote schaal verzamelen van gegevens (Van Est et al. 2016). Op dat vlak gaat het met name om privacy. Voor dat thema is ook vanuit regulering en toezicht traditioneel veel aandacht. Denk bijvoorbeeld aan de Wet bescherming persoonsgegevens (Wbp), de meldplicht datalekken en de Europese dataprotectieverordening. In de toekomst blijft data verzamelen een belangrijk onderwerp aangezien monitoring door de opkomst van het IoT, robotica en biometrie naar een nieuw niveau wordt getild.

Naast het verzamelen van gegevens roepen de analyse, en toepassing van data inmiddels vele vragen op. Als we het hebben over profilering komen we in het domein van de analyse terecht. Hier hangen vraagstukken mee samen op het gebied van rechtvaardigheid en discriminatie. Evenals de zorgen over de ondoorzichtigheid van die analyses. Controle en toezicht op algoritmes wordt steeds belangrijker naarmate ze in steeds meer domeinen (op de weg, gezondheidszorg, rechtspraak, e-commerce) worden ingezet om beslissingen te ondersteunen, of zelfs over te nemen.

Daarmee maken we de stap naar de derde fase van de cybernetische loop, de toepassing. Hier komen we op het niveau van de interventies terecht, en krijgen we te maken met de vraagstukken omtrent individuele autonomie en de controleerbaarheid van technologie. In hoeverre keuzes voor ons voorgesorteerd en genudged worden door software, welke taken we uit willen besteden aan robotica en welke niet, wat er nog overblijft aan menselijk werk en wat dat betekent voor menselijke waardigheid. Naast het verzamelen van gegevens lijken de nieuwe uitdagingen van digitalisering voor de komende jaren dus juist op het vlak van de analyse en toepassing van die digitale gegevens te liggen.

Als we kijken naar het geheel van de hier beschreven kwesties wordt duidelijk dat de impact van digitalisering niet onderschat kan worden. Het perspectief dat de impact van digitalisering om aandacht vraagt, wordt onderstreept doordat de centrale ethische thema's samenhangen met belangrijke waarden die zijn vastgelegd in internationale verdragen en de Nederlandse Grondwet. Kwesties zoals privacy en rechtvaardigheid zien we onder andere terug in het recht op eerbiediging van de persoonlijke levenssfeer, het recht op gelijke behandeling en het recht op een eerlijk proces. Menselijke waardigheid en veiligheid zijn geen onderdeel van de Nederlandse Grondwet maar worden wel benoemd in internationale verdragen zoals het Handvest van de grondrechten van de Europese Unie (EU-Handvest) en de Universele Verklaring van de Rechten van de Mens (UVRM). Waarden zoals autonomie, gelijke machtsverhoudingen en controle over technologie worden niet expliciet benoemd in verdragen maar kunnen worden gezien als onderdeel van of volgend uit deze

grond- en mensenrechten. Digitalisering raakt dus belangrijke publieke waarden. Dat maakt ook de governance van deze ethische en maatschappelijke vraagstukken tot een belangrijke uitdaging.

# 4 Governance in historisch perspectief

## 4.1 Inleiding

Wetenschap en technologie worden in de westerse samenleving gezien als belangrijke bronnen van economische en maatschappelijke vooruitgang, maar leiden ook vaak tot publieke en politieke discussies over bijvoorbeeld fysieke risico's of ethische grenzen. Voorbeelden hiervan zijn discussies over onderzoek met menselijke embryo's of genetische modificatie van voedsel en dieren. Deze onderwerpen hebben diverse malen geleid tot reflectie vanuit de overheid over de manier waarop op een systematische wijze kan worden omgegaan met ethische en maatschappelijke kwesties die samenhangen met nieuwe technologische mogelijkheden. Daarbij kwam steeds de vraag naar voren in hoeverre de bestaande institutionele inbedding adequaat is dan wel aanscherping behoeft.

In dit hoofdstuk willen we zicht krijgen op hoe we in algemene zin het *governance-ecosysteem* van maatschappelijke en ethische kwesties die ontstaan door technologie kunnen begrijpen. Kader 4.1 licht de betekenis van het begrip governance toe. We richten ons vooral op de *structuur en werking* van het governance-ecosysteem, en de rol van commissies daarin. We doen dit door een historisch overzicht te maken van hoe we in Nederland de afgelopen halve eeuw politiek-bestuurlijk en maatschappelijk zijn omgegaan met maatschappelijke en ethische kwesties rond vier technologische ontwikkelingen: ICT, biotechnologie, medisch-wetenschappelijk onderzoek met menselijke proefpersonen (mensgebonden onderzoek) en met dieren (dierexperimenten).<sup>58</sup> Deze vier thema's dekken niet alle wetenschappelijke en technologische ontwikkelingen die maatschappelijke en ethische vragen oproepen. Maar de beschrijving is breed genoeg om een algemeen conceptueel kader op te stellen over een governance-ecosysteem van ethische en maatschappelijke kwesties rond technologische ontwikkelingen. Het historisch overzicht laat tevens zien wat voor soort commissies in het verleden zijn ingesteld op de vier gebieden, wat voor commissies dat waren, en welke rol zij vervulden in dit ecosysteem. In het volgende hoofdstuk gebruiken we dit conceptuele kader om te zien hoe het governance-ecosysteem van ethische en maatschappelijke kwesties rond digitalisering op dit moment vorm krijgt.

We beschrijven de vier technologische gebieden op chronologische wijze, van decennium naar decennium. Om te zorgen dat de lezer zicht houdt op de samenhang tussen de vele gebeurtenissen door de jaren heen, verwijzen we regelmatig naar gebeurtenissen die een decennium eerder of later plaatsvinden.

---

<sup>58</sup> Het Rathenau Instituut is sinds 1986 onderdeel van het governance-ecosysteem rond maatschappelijke en ethische kwesties van technologie. Het Instituut heeft als taak publieke en politieke meningsvorming over wetenschap en technologie te stimuleren. In de analyse van het ecosysteem rond de vier technologische gebieden benoemen we daarom ook de activiteiten van het Rathenau Instituut.



#### Kader 4.1 De betekenis van publieke governance

Governance is een meerduidig concept dat in omvangrijke literatuur wordt beschreven. In Appendix B introduceren we verschillende inzichten en begrippen uit die literatuur die relevant zijn voor de aanpak van deze studie. In dit kader vatten we enkele van die begrippen kort samen.

Governance is gericht op het aanpakken van publieke problemen. Dat zijn problemen die slechts via collectieve actie opgelost kunnen worden (vgl. Hoppe 2010). Het gaat daarbij enerzijds om het vinden en agenderen van problemen en anderzijds om het oplossen daarvan. Het begrip governance impliceert dat de overheid niet als enige behartiger van publieke belangen gezien wordt en dat sturing van de samenleving niet alleen plaatsvindt via formele instrumenten, zoals wet- en regelgeving. De overheid opereert niet geïsoleerd, maar samen met anderen in meer horizontale verhoudingen (NSOB & PBL 2014). De overheid is dus een netwerkpartner en stuurt in interactie met andere partijen. Ze maakt daarbij gebruik van een mix van diverse formele en informele praktijken, zoals stimulering van publiek debat, onderhandelingen, samenwerking, gezamenlijke visievorming en vorming van allianties (cf. Van Kersbergen & Van Waarden 2004, pp. 151-152).

Diverse governance-begrippen verwijzen naar bepaalde typen van interactie tussen de overheid en maatschappelijke actoren. Vormen van governance zijn onder meer van *multi-stakeholder governance* of *netwerk governance*, *multi-level governance* en *deliberatieve governance* (Hajer et al. 2004). Bij *netwerk governance* ontwikkelen actoren uit het bedrijfsleven, de maatschappij en de overheid een gezamenlijke aanpak voor een kwestie die hen allen aangaat, maar te complex is om zonder samenwerking effectief aan te pakken. Bij *netwerk governance* vindt er meer horizontale afstemming plaats tussen stakeholders en worden gezamenlijke besluiten vastgelegd in 'akkoorden' (NSOB & PBL 2014, p. 21). Naast interactie tussen publieke en private actoren, vragen vele kwesties ook om overleg tussen diverse bestuurslagen, zoals Europees, nationaal, regionaal en lokaal. Dit wordt *multi-level governance* genoemd. Daar waar het specifiek gaat om de interactie tussen overheidspartijen, burgers en maatschappelijke groepen gebruikt men vaak de term *deliberatieve governance*.

In Nederland werkt de overheid al zeer lang samen met diverse actoren uit de samenleving. De afgelopen decennia is de behoefte aan governance gegroeid vanwege digitalisering, privatisering en internationalisering (Hajer et al. 2004). Governance kan ook een reactie zijn op publiek verzet, gebrek aan draagvlak, institutioneel wantrouwen of de complexiteit van vraagstukken.

Governance draait dus niet alleen om het handelen van de overheid. Het is daarom van belang om oog te hebben voor het gehele systeem aan governance-arrangementen in de samenleving om publieke problemen te agenderen en daarvoor oplossingen te vinden. Dat vraagt om een diverse set aan instituties en bestuurlijke en maatschappelijke processen.

Tezamen vormt die set een zogeheten governance-ecosysteem: het geheel aan governance-arrangementen rondom een bepaald publiek probleem. Hoppe (2004) spreekt van *meta-governance* omdat het hier gaat om de governance van de governance van problemen, oftewel de inrichting van het governance-ecosysteem waarmee collectieve problemen benoemd en geadresseerd kunnen worden.

Voor onze aanpak is het onderscheid tussen governance en meta-governance van belang. Met betrekking tot de governance gaat het om vragen als: Welke publieke problemen zijn gesignaleerd? Welke belangen of waarden zijn goed of minder goed gearticuleerd? Hoe discussiëren burgers en politici over deze problemen? Hoe zijn problemen al dan niet politiek geagendeerd? Welke partijen zijn betrokken geweest bij het debat en de vormgeving van beleid? Welke oplossingen zijn aangedragen en geïnstitutionaliseerd?

Met betrekking tot de meta-governance gaat het om vragen als: Welke instituties zijn er om te discussiëren over publieke problemen en deze politiek aan te kaarten? Op welke manieren vindt afstemming plaats tussen publieke en private actoren en tussen overheden, burgers en maatschappelijke organisaties? Op welke wijze worden publieke waarden institutioneel geborgd? Welke instituties zijn er door de jaren heen opgebouwd om dat te doen? Hoe ziet het governance-ecosysteem rond een bepaalde kwestie er uit?

## 4.2 Jaren 1970: maatschappelijke en ethische zorgen over wetenschap en technologie

### **Biotechnologie: recombinant DNA-technologie en de Brede DNA Commissie**

In de jaren zeventig groeide op verschillende fronten de kritiek op wetenschap en technologie. De uitvinding van recombinant-DNA-technologie leidde na de Asilomar-conferentie in 1975 tot ethische discussies in kleine kring. In reactie stelde de Nederlandse regering de Brede DNA Commissie (1981-1983) op om zich te buigen over de mogelijke toepassingen en over maatschappelijke en ethische aspecten van recombinant-DNA-onderzoek. We zullen zien dat de bio- of gentechnologie de gemoederen tot op de dag van vandaag bezighouden.

### **Dierexperimenten: Wet op de dierproeven**

In de loop van twintigste eeuw nam het gebruik van dieren binnen de biomedische wetenschappen enorm toe (Swart et al. 2004). In 1908 waren bij dierproeven minder dan vijfduizend dieren betrokken, in 1978 circa anderhalf miljoen. Om deze trend te keren werd in 1977 de Wet op de dierproeven (Wod) aangenomen. Beschermwaardigheid van het dier werd het uitgangspunt van deze wet. De wet bepaalde dat inrichtingen voor dierproeven een vergunning moesten hebben. Om in aanmerking te komen voor een vergunning moest een inrichting voldoen aan verschillende verplichtingen: de registratie van dierproeven en proefdieren, het formuleren van deskundigheidseisen voor onderzoekers, biotechnici en dierverzorgers, en het aanstellen van een deskundige die toezicht houdt op het welzijn van de proefdieren (Swart et al. 2004). De opbouw van dit systeem nam twee decennia in beslag. Als onderdeel van dat proces richtten tal van

vergunninghouders begin jaren tachtig vrijwillig een interne Dierexperimentencommissie (DEC) op.<sup>59</sup>

### **ICT: privacy als nieuw grondrecht, de Wet persoonsregistratie en de commissie Rathenau**

De volkstelling in 1971 veroorzaakte een heftige maatschappelijke discussie over privacy. Dat leidde tot een staatscommissie Cals/Donner (1967-1971) en uiteindelijk in 1983 tot een grondwetswijziging waarbij privacy als een grondrecht toegevoegd (artikel 10). Deze grondwetswijziging legde de basis voor de Wet persoonsregistratie in 1988.<sup>60</sup> Om toe te zien op de uitvoering van deze wet werd de Registratiekamer opgericht.<sup>61</sup>

Aan het einde van de jaren zeventig leidde de opkomst van de micro-elektronica (onder meer in de PC) tot brede maatschappelijke zorgen over de werkgelegenheid. In 1978 en 1979 onderzocht een commissie onder leiding van prof. dr. G.W. Rathenau de maatschappelijke gevolgen van micro-elektronica. Een van de aanbevelingen van de commissie was de wens om de maatschappelijke betekenis van nieuwe technologie systematisch te gaan bestuderen, in jargon technology assessment geheten. De Commissie Rathenau legde daarmee de basis voor de oprichting in 1986 van de Nederlandse Organisatie voor Technologisch Aspectenonderzoek (NOTA, nu het Rathenau Instituut) (zie volgende paragraaf).

## **4.3 Jaren 1980: institutionalisering van maatschappelijke en ethische omgang met wetenschap en technologie**

Bovengenoemde discussies over specifieke technologieën zorgden in de jaren tachtig ook voor politiek-bestuurlijke aandacht voor de vraag hoe in het algemeen maatschappelijke en ethische kwesties systematisch in wetenschaps- en technologiebeleid konden worden verankerd. Het eerste Kabinet-Lubbers (1982-1986) legde in het regeerakkoord vast dat maatschappelijke en ethische consequenties van technologische vernieuwingen beter zichtbaar moesten worden gemaakt (Kamerstukken II 1982-1983, 17555, nr. 7, p. 87). Dit leidde in 1984 tot de Nota 'Integratie van Wetenschap en Technologie in de Samenleving' (IWTS-nota; Kamerstukken II 1983-1984, 18424, nr. 2) met als belangrijkste doelstellingen een structurele inbedding van Technology Assessment (TA) in het beleid en meer aandacht voor voorlichting en opinievorming over wetenschap en technologie. Hieruit volgde in 1986 de oprichting van de Nederlandse Organisatie voor Technologisch Aspectenonderzoek (NOTA, in 1994 omgedoopt in Rathenau Instituut). NOTA kreeg de taak onderzoek te doen naar maatschappelijke en ethische aspecten van wetenschap en technologie, om zo de politiek te informeren, maar ook om de publieke discussie over nieuwe

---

<sup>59</sup> Met het Dierproevenbesluit trad in het midden van de jaren tachtig de Wod in haar volle omvang in werking. De Wod voorzag tevens in een permanente Commissie van Advies voor de Dierproeven, die tot taak had de regering op dit terrein te adviseren en de publieke discussie te bevorderen.

<sup>60</sup> Sinds 2001 is de opvolger de Wet bescherming persoonsgegevens (Wbp). Sinds 2001 werd de opvolger daarvan, de Wet bescherming persoonsgegevens (Wbp), van kracht. De Wbp is de Nederlandse uitwerking van de Europese richtlijn bescherming persoonsgegevens (95/46/EG).

<sup>61</sup> Sinds 2001 het College Bescherming Persoonsgegevens (CBP) en sinds 2016 de Autoriteit Persoonsgegevens (AP). De AP staat voor het grondrecht op bescherming van persoonsgegevens en houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving

ontwikkelingen te stimuleren. In 1986 werd ook de Stichting voor Publieksvoorlichting over Wetenschap en Technologie (Stichting PWT) opgericht.<sup>62</sup>

### **Dierenexperimentencommissies (DECs)**

Naar aanleiding van de Wet op de dierproeven (Wod) uit 1977 werden begin jaren tachtig dierexperimentencommissies (DECs) opgericht als een vorm van zelfregulatie. In de loop van de jaren tachtig groeide de behoefte aan uniforme voorwaarden voor een onafhankelijk ethisch beslisproces (Van Boxsel 1991). In 1985 adviseerde de Commissie van Advies voor de Dierproeven over de wettelijke inbedding van DECs (Swart et al. 2004). De Wod werd in 1996 gewijzigd naar aanleiding van EU-regelgeving, en daarmee werden DECs geformaliseerd. Een DEC toetst onder meer of het lijden van de proefdieren opweegt tegen het doel van de proef. Terwijl in 1977 de Wod draaide om de beschermwaardigheid van het dier, werd in 1996 de intrinsieke waarde van het dier het algemeen uitgangspunt van de Wod (Swart et al. 2004). Het advies van een DEC is bindend. Bij een negatief advies kan de vergunninghouder het onderzoeksvorstel voor een second opinion voorleggen aan de Centrale Commissie Dierproeven (CCD). Indien deze ook negatief oordeelt mag de dierproef niet worden uitgevoerd.<sup>63</sup>

### **Medisch-ethische toetsingscommissies (METCs)**

Naar Amerikaans voorbeeld stelden begin jaren zeventig enkele academische ziekenhuizen in Nederland op eigen initiatief medisch-ethische toetsingscommissies (METCs) in. In de tweede helft van de jaren tachtig nam het aantal instellingen met een METC drastisch toe, maar er was een gebrek aan uniforme criteria voor ethische toetsing (Van Boxsel 1991). Vanuit het veld was er behoefte aan een onafhankelijk orgaan 'op afstand', dat een second opinion zou kunnen geven bij de toetsing van medisch-wetenschappelijke onderzoeksvorstellen waaraan bijzonder ethische, juridische en maatschappelijke vraagpunten verbonden waren (KEMO 2004). Eind jaren tachtig was in het ontwerp van de Wet medisch-wetenschappelijk onderzoek met mensen (Wmo) al een dergelijke commissie voorzien. In 1989 werd de Kerncommissie Ethiek Medisch Onderzoek (KEMO) opgericht. Tien jaar en 27 adviezen later werd de KEMO daadwerkelijk opgevolgd door de Centrale Commissie Mensgebonden Onderzoek (CCMO). De CCMO heeft diverse toetsingstaken in het kader van de Wmo (1998) en de Embryowet (2002). De CCMO houdt toezicht op de werkzaamheden van decentrale, erkende METCs.

---

<sup>62</sup> Op 1 januari 1997 fuseerde de Stichting PWT en Stichting Wetenschapsweek en Techniek in de Stichting Weten, die op 1 januari 2005 werd opgeheven.

<sup>63</sup> Eind 2014 werd de Europese Richtlijn (2010/63/EU), die betrekking heeft op dierproeven in wetenschappelijk onderzoek, ingevoerd in onze nationale wetgeving. Hierdoor is het organisatorische model voor de beoordeling van dierproeven gewijzigd. Twee organisaties spelen daarbij een rol: de landelijke Centrale Commissie Dierproeven (CCD) en het Nationaal Comité advies dierproevenbeleid (NCad). De CCD is het centrale orgaan dat als enige bevoegd is om projectvergunningen voor het uitvoeren van dierproeven te verlenen. Het NCad is ingesteld voor de bescherming van dieren die worden gebruikt voor wetenschappelijke doeleinden en voor onderwijs. Het NCad wil zowel nationaal als internationaal het proefdiergebruik minimaliseren door het vervangen van dierproeven door diervrije methoden van onderzoek, het verminderen van het aantal proefdieren in onderzoek en het verminderen van het ongerief van proefdieren.

## 4.4 Jaren 1990: vermaatschappelijking en regulering van de bio-ethiek

### Vermaatschappelijking van de gentechologie

In de jaren negentig laaiden in Nederland en internationaal tal van discussies rondom de toepassing van biotechnologie op. In de jaren zeventig leidde de uitvinding van recombinant-DNA-technologie tot discussie in kleine kring. In de jaren negentig brachten verschillende concrete toepassingen van genetische technologie de biotechnologie onder de aandacht van een breder publiek.<sup>64</sup> Naast genetische modificatie van micro-organismen kwam de toepassing van gentechologie voor planten, dieren en mensen onder de aandacht. Een bekende mijlpaal die veel aandacht trok was bijvoorbeeld de geboorte in 1990 van Nederlandse stier Herman, de eerste transgene stier ter wereld.<sup>65</sup> In dit decennium veranderde biotechnologie van iets dat in het lab gebeurde tot iets dat op allerlei manieren maatschappelijke betekenis heeft.

Tegelijkertijd stonden wetenschappelijke ontwikkelingen op dit gebied niet stil. Maatschappelijke discussies ontstonden rond het gebruik van genetisch gemodificeerde proefdieren, onderzoek met menselijke embryo's, het in kaart brengen van het menselijke genoom en het klonen van dieren en mensen. In de eerste helft van de jaren negentig ontstond er vanuit het perspectief van mensenrechten en internationale organisaties veel aandacht voor ontwikkelingen in de humane genetica (zie kader 4.2). Om de ontwikkelingen van genetische modificatie in Nederland te begeleiden werd in 1990 de (Voorlopige) Commissie Genetische Modificatie opgericht en in 1992 de Voorlopige Commissie Ethische Toetsing Genetische Modificatie van Dieren (later Commissie Biotechnologie bij Dieren).

### Commissie Genetische Modificatie en Commissie Biotechnologie bij Dieren

In 1990 werd de Voorlopige Commissie Genetische Modificatie (VCOGEM) opgericht, die in 1998 werd opgevolgd door de huidige Commissie Genetische Modificatie (COGEM). De taken van de COGEM zijn vastgelegd in de Wet Milieubeheer. De COGEM adviseert de regering over mogelijke risico's van productie en handelingen met genetisch gemodificeerde organismen (ggo's) voor mens en milieu. Ook informeert de COGEM de regering op verzoek van de minister van Infrastructuur & Milieu of uit eigen beweging over ethisch-maatschappelijke aspecten verbonden aan genetische modificatie. Dit gebeurt via signaleringen.

In 1992 stelde de minister van Landbouw, Natuurbeheer en Visserij de Voorlopige Commissie Ethische Toetsing Genetische Modificatie van Dieren in, in het kader van de nieuwe Gezondheids- en welzijnswet voor dieren (GWWD). Deze voorlopige commissie moest adviseren over de toelaatbaarheid vanuit ethisch oogpunt van onderzoeksprojecten op het terrein van de genetische modificatie van dieren.<sup>66</sup> In 1997 werd deze voorlopige commissie door middel van het Besluit

---

<sup>64</sup> In 1982 was de eerste synthetische humane insuline op de markt gebracht die met behulp genetisch gemodificeerde E. coli-bacteriën was gemaakt, waarin met recombinant-DNA-technologie menselijk DNA was ingebracht.

<sup>65</sup> Andere voorbeelden zijn het eerste gebruik van gentherapie bij mensen in 1991 in Italië en de introductie van het eerste genetisch gemodificeerde voedsel op de Amerikaanse markt in 1994 en twee later in Groot-Brittannië

<sup>66</sup> Dit naar aanleiding van de maatschappelijk en ethische discussies over het gebruik van biotechnologie bij dieren (gestimuleerd door de geboorte van de genetisch gemodificeerde stier Herman in 1990).

Biotechnologie geformaliseerd in de Commissie Biotechnologie bij Dieren (CBD). De CBD adviseerde of vergunningen voor genetische modificatie bij dieren konden worden toegestaan. Elke individuele vergunningaanvraag onderging een ethische toets om te bepalen of voldaan werd aan de in wet genoemde voorwaarden. De CBD had als een tweede doel inzicht te krijgen welke biotechnologische handelingen bij dieren voor biomedisch onderzoek ethisch aanvaardbaar zijn.<sup>67</sup>

#### **Kader 4.2: Internationale bio-ethische verdragen vanuit mensenrechtenperspectief**

##### *Raad van Europa en het Verdrag van Oviedo*

In de eerste helft van de jaren negentig ontstond er vanuit het perspectief van mensenrechten en internationale organisaties aandacht voor ontwikkelingen in de humane genetica. De Parlementaire Vergadering van de Raad van Europa beval in 2001 een Verdrag inzake bio-ethiek voor te bereiden. Die kreeg in 1997 zijn beslag in het Verdrag inzake de rechten van de mens en de biogeneeskunde (Verdrag van Oviedo) opgesteld.<sup>68</sup> Ondanks het brede toepassingsbereik van het Europees Verdrag voor de Rechten van de Mens (EVRM) achtte de Raad van Europa het noodzakelijk om zich expliciet te richten tot wetenschappelijke en technologische ontwikkelingen; er moest worden gezocht naar een balans tussen vooruitgang en menselijke waardigheid. Artikel 1 beschrijft het doel van het verdrag: 'De Partijen bij dit Verdrag beschermen de waardigheid en identiteit van het menselijk wezen en waarborgen iedereen, zonder onderscheid, dat zijn integriteit en andere rechten en fundamentele vrijheden met betrekking tot de toepassing van de biologie en de geneeskunde worden geëerbiedigd.' Het verdrag beperkte zich tot algemene principes. Additionele standaarden en specifieke kwesties moesten geregeld worden in additionele protocollen. Zo werd snel na het nieuws rondom het schaap Dolly, in 1998, het eerste additionele protocol opgesteld, waarin het kloneren van mensen werd verboden.

##### *UNESCO Universal Declaration on Bioethics and Human Rights*

Naast de Raad van Europa, boog ook de United Nations Educational, Scientific and Cultural Organization (UNESCO) zich over de ontwikkelingen in de genetica. In 1993 werd de UNESCO door haar lidstaten gemandateerd om op het gebied van de bio-ethiek standaarden en grenzen te formuleren (Andorno 2006). Na enkele doorbraken in de ontrafeling van het menselijk genoom, werd in 1997 de Universal Declaration on the Human Genome and Human Rights door de Algemene Vergadering van de UNESCO aangenomen. In 2003 volgde de International Declaration on Human Genetic Data. Daarnaast bleek er behoefte aan een juridisch instrument met een meer algemene bio-ethische strekking en dus

<sup>67</sup> In 2008 besloot de Tweede Kamer dat de toetsing niet tot nieuwe inzichten op dit punt zou leiden en vereenvoudigde de regelgeving. Sinds 2010 kan worden volstaan met een toets in het kader van de Wet op de dierproeven. Er bleef wel een vergunning nodig voor biotechnologische handelingen bij dieren die niet bestemd zijn voor biomedische doeleinden, zoals voor voedselproductie. Hierbij bleef de CBD betrokken. In 2014 werd de CBD opgeheven. (wetten.overheid.nl/BWBR0008392/2005-07-01)

<sup>68</sup> Momenteel hebben 29 lidstaten van de Raad van Europa het Verdrag van Oviedo geratificeerd. Zes lidstaten, waaronder Nederland, hebben het Verdrag ondertekend, maar nog niet geratificeerd. De Nederlandse tekst van het verdrag is in te zien op: [coe.int/t/dg3/healthbioethic/texts\\_and\\_documents/ETS164Dutch.pdf](http://coe.int/t/dg3/healthbioethic/texts_and_documents/ETS164Dutch.pdf)

een grotere reikwijdte dan humane genetica. Die behoefte leidde in 2005 tot de UNESCO Universal Declaration on Bioethics and Human Rights. Volgens de UNESCO (2005) was het opportuun en wenselijk 'to set universal standards in the field of bioethics with due regard for human dignity and human rights and freedoms, in the spirit of cultural pluralism inherent in bioethics' (UNESCO 2005). Twee jaar later werd deze verklaring unaniem aangenomen door de lidstaten van de UNESCO.

### **Behoeftte aan wettelijke verankering ethische commissies**

Zoals hierboven beschreven groeide in de jaren tachtig het aantal lokale medisch-ethische commissies (METCs) en ethische commissies voor experimenten met dieren (DECs) flink. In 1990 ontstond er in de Tweede Kamer onduidelijkheid over het aantal, de werkwijzen van, en de samenwerking tussen dergelijke ethische commissies. De Kamer vroeg zich af of via al die commissies de ethische en maatschappelijke aspecten wel adequaat werden meegenomen in de besluitvorming. Via de motie Laning-Boersema vroeg de Kamer daarom het toenmalige ministerie van Onderwijs en Wetenschappen (nu het ministerie van Onderwijs, Cultuur en Wetenschappen) een kader te ontwikkelen voor ethische discussies en de beoordeling daarvan (Kamerstukken II 1989-1990, 21319, nr. 6). Dit leidde in 1991 tot de Nota 'Kader voor discussies over ethische aspecten van wetenschappelijk onderzoek' (Kamerstukken II 1990-1991, 21319, nr. 12) (zie kader 4.3).

#### **Kader 4.3 Nota 'Kader voor discussies over ethische aspecten van wetenschappelijk onderzoek'**

##### *Vier manieren om ethische aspecten aandacht en vorm te geven*

Minister Ritzen onderscheidde vier manieren waarop ethische en maatschappelijke aspecten aandacht en vormgeving kunnen krijgen: signalering, articulatie, gezaghebbende toedeling van waarden en analyse en fundering van waarden (Kamerstukken II 1990-1991, 21319, nr. 12). De minister gaf ook aan dat de fora waarin op een gezaghebbende wijze (bindende) uitspraken gedaan kunnen worden over ethische kwesties verschillen van zeer geformaliseerd (wetgever en wetgeving) tot situatiegebonden (bijvoorbeeld medisch-ethische commissies die per geval een uitspraak doen) of meer algemeen (incidentele commissies, zoals de eerder genoemde Brede DNA Commissie).

##### *Signalering*

Groepen in de samenleving maken kenbaar dat zij menen dat bepaalde normen en waarden door wetenschappelijke en technologische ontwikkelingen onder druk komen te staan. Ze verwoorden hun ongerustheid en trachten deze onder de aandacht te brengen van instanties die naar hun mening in staat zijn zo'n vraagstuk ter hand te nemen. Daarmee wordt het signaal gegeven dat er een probleem is.

##### *Articulatie*

In een tweede fase van dit proces gaan organisaties als de NOTA een rol spelen die zulke bewegingen in kaart brengen en aangeven in welke discussiepunten de vraagstukken uiteen te zetten zijn. Daarmee wordt het probleem gearticuleerd.

*Gezaghebbende toedeling van waarden door overheid en andere partijen*

In de maatschappelijke en politieke discussie wordt tussen de betrokken groepen overeenstemming bereikt over welk forum het gezag krijgt om over de ethische probleemgebieden een bindende uitspraak te doen. Vervolgens worden zulke uitspraken gedaan. Het forum en de wijze waarop het uitspraken doet, kunnen zeer geformaliseerd zijn (wetgever en wetgeving), situatiegebonden (medisch-ethische commissies die per geval een uitspraak doen) of meer algemeen (incidentele commissies zoals de Brede DNA commissie). Deze processen worden gevoed met de resultaten van ethisch-wetenschappelijk onderzoek.

*Analyse en fundering van waarden*

Hierbij gaat het om ethisch/filosofisch onderzoek, waarbij de fundering en de inhoud van waarden kritisch worden beschouwd. Dit is het terrein waarop vooral filosofen, ethici en theologen zich bewegen.

### **Behoeftte aan maatschappelijk debat over bio-ethische kwesties**

De regering hechtte in de jaren negentig waarde aan het maatschappelijke debat over ethische kwesties die kunnen spelen rondom nieuwe technologische ontwikkelingen. In 1994 installeerde minister Ritzen bij het Rathenau Instituut het Platform Wetenschap en Ethiek voor een experimentele periode van drie jaar. Dit platform had als doel om maatschappelijke discussies over ethische aspecten van wetenschappelijk onderzoek te stimuleren. Het experiment werd met een jaar verlengd en in 1997 geëvalueerd. De platformfunctie werd daarna structureel bij het Rathenau Instituut belegd.

Vanaf 1998 werden binnen een tijdsbestek van vijf jaar drie publieke debatten op het gebied van biotechnologie georganiseerd. In 1998 verzocht toenmalig minister van Volksgezondheid Borst het Rathenau Instituut een maatschappelijk debat over klonen te organiseren. Ze deed dit na de ophef die ontstond toen Schotse wetenschappers er in slaagden een schaap te klonen (Dolly). In 1999 startte een voorlichtingscampagne en publiek debat over xenotransplantatie,<sup>69</sup> naar aanleiding van een advies van de Gezondheidsraad over de maatschappelijke en ethische aspecten van xenotransplantatie, en de kabinetsreactie daarop (Kamerstukken II 1998-1999a, 26335, nr. 1).<sup>70</sup> De Stichting Consument en Biotechnologie organiseerde deze campagne en het debat (Kamerstukken II 1998-1999b, 26335, nr. 3). Ten slotte startte in 2001 het publieke debat 'Eten en genen' over de maatschappelijke en ethische kwesties rondom biotechnologie en voedsel (Commissie Terlouw, TK stukken 2000-2001b, 27248, nr. 3). Het doel van de Tijdelijke Commissie Terlouw was het vergroten en uitwisselen van informatie over biotechnologie en voedsel onder een zo breed

<sup>69</sup> Bij xenotransplantatie kunnen organen of weefsels van verschillende soorten worden ingebracht (meestal tussen mens en dier).

<sup>70</sup> Toenmalig minister Borst van Volksgezondheid, Welzijn en Sport verzocht eind december 1996 de Gezondheidsraad om dit advies.



mogelijk publiek, het bieden van mogelijkheden tot discussie en meningsvorming en het vastleggen van de uitkomsten van het publieke debat.

### **Aandacht voor de invloed van ICT op de samenleving**

In de tweede helft van de jaren negentig ontstond met de opkomst van het internet ook aandacht voor de groeiende invloed van ICT op de maatschappij. Het Kabinet-Kok II (1998-2002) wilde tijdens de kabinetsperiode een visie vormen over de rol van de overheid in de informatiesamenleving. In 1999 werd daarom het programmabureau Infodrome opgericht. Infodrome moest de maatschappelijke gevolgen van grootschalige toepassing van ICT inventariseren en analyseren, en vervolgens aangeven welke implicaties die veranderingen konden hebben voor de rol van de overheid. Infodrome werd geleid door de Stuurgroep Infodrome, die onder voorzitterschap stond van Rick van der Ploeg, de staatssecretaris van Onderwijs, Cultuur en Wetenschappen. In december 2001 werd het eindrapport van Infodrome aan het parlement aangeboden getiteld *Controle geven of nemen: Een politieke agenda voor de informatiesamenleving*.

In juli 1999 werd ook de staatscommissie 'Grondrechten in het digitale tijdperk' ingesteld, onder leiding van prof. dr. H. Franken. Het besluit tot deze commissie volgde na discussies over het mogelijk wijzigen van het grondrecht op het briefgeheim. Naar aanleiding van de dissertatie van Hofman waarin een techniek-onafhankelijk perspectief op 'vertrouwelijke communicatie' werd bepleit, diende de regering in 1997 een wetsvoorstel tot wijziging van het grondrecht op het briefgeheim in (Kamerstukken II 1996-1997, 25 443, nr. 1/2). Het voorstel werd vanuit meerdere hoeken bekritiseerd en uiteindelijk ingetrokken (Kamerstukken II 1998-1999, 25 443, nr. 40). De daarna ingestelde commissie (Commissie Franken) kreeg tot taak kreeg aanbevelingen te doen over aanpassing van de grondrechten in relatie tot ontwikkelingen in de informatietechnologie (Nouwt et al. 2000). De Commissie Franken kwam in 2000 met haar rapport waarin ze zich richt op aanpassing van artikel 7 (vrijheid van meningsuiting), artikel 10 (eerbiediging persoonlijke levenssfeer) en artikel 13 (vertrouwelijke communicatie). Het doel was om deze artikelen op een technologie-neutrale en toekomstbestendige manier te formuleren. De adviezen van de Commissie Franken werden grotendeels overgenomen door het kabinet (Tweede Kamer 2000-2001, 27460, nr.1), maar stuitte op scherpe kritiek van de Raad van State in 2004, waarop werd besloten de voorstellen in te trekken (Verhey 2011; Koops 2011).<sup>71</sup>

## **4.5 Jaren 2000: onderzoek, signalering en debat over ethiek en bio- en nanotechnologie**

### **Behoefte aan integraal bio-ethisch toetsingskader**

Na afronding van het publieke debat 'Eten en genen' volgde in 2002 de behandeling van de Integrale Beleidsnota Biotechnologie (Kamerstukken II 2000-2001a, 27428, nr. 2). In deze nota werd gezocht naar een balans tussen kansen voor innovatie en mogelijke negatieve gevolgen.

---

<sup>71</sup> In 2009 werd er wederom een staatscommissie ingesteld, de Commissie Thomassen, om, mede in het licht van digitalisering, te adviseren over mogelijke herziening van onze grondrechten

Veiligheid en maatschappelijk-ethische aanvaardbaarheid werden als randvoorwaarden voor toepassingen in biotechnologie geformuleerd.

In de Tweede Kamer bleek bij veel partijen de behoefte te bestaan aan een integraal ethisch toetsingskader voor toepassingen in de biotechnologie, uitgaande van de intrinsieke waarden van leven, ecologische duurzaamheid en biodiversiteit. Dit kader 'Verantwoord en zorgvuldig toetsen' werd in 2003 opgesteld (Kamerstukken II 2002-2003, 27428, nr. 39). In 2003 werd ook het Centrum voor Ethiek en Gezondheid (CEG) opgericht. Het CEG was een samenwerkingsverband tussen enerzijds de Gezondheidsraad en anderzijds de toenmalige Raad voor de Volksgezondheid en Zorg (RVZ)<sup>72</sup> (zie kader 4.4). Het CEG signaleert en informeert over nieuwe ontwikkelingen op het gebied van ethiek, gezondheid en beleid. Jaarlijks stuurt het CEG signaleringsrapporten over medisch-ethische ontwikkelingen naar het ministerie van VWS. Deze rapporten zijn input voor de agenda Ethiek en Gezondheid, die ieder jaar bij de Rijksbegroting worden aangeboden en in de Tweede Kamer worden besproken. Verder is het CEG een informatiepunt voor ethische kwesties op het gebied van de volksgezondheid.

#### **Kader 4.4. Gezondheidsraad en Raad voor Volksgezondheid en Samenleving (RVS)**

##### *Gezondheidsraad*

De Gezondheidsraad (opgericht in 1902) informeert de regering onder andere over ethische onderwerpen met betrekking tot biotechnologie. De Gezondheidsraad is een van de adviesorganen van de Nederlandse overheid en heeft als taak ministers en parlement te adviseren over de stand van zaken binnen de wetenschap op het gebied van de volksgezondheid en gezondheids(zorg)onderzoek. Daarnaast heeft de Gezondheidsraad een signalerende taak en kan daardoor de overheid ongevraagd adviseren. De adviezen van de Gezondheidsraad dienen als onderbouwing voor het overheidsbeleid en worden samengesteld op basis van zowel technisch-wetenschappelijke overwegingen als ethisch-maatschappelijke overwegingen (Zoeteman & Widdershoven-Heerdink 2007).

##### *Raad voor de Volksgezondheid en Samenleving*

De Raad voor de Volksgezondheid en Samenleving (RVS) is net als de Gezondheidsraad een van de officiële adviesorganen van de Nederlandse regering. De RVS is opgericht in 2015 en is een samenvoeging van de Raad voor Maatschappelijke Ontwikkeling en de Raad voor de Volksgezondheid en Zorg. De RVS heeft tot taak strategische adviezen te geven over het te voeren beleid over 'alle aspecten die van invloed zijn op de gezondheid en het functioneren van burgers in de samenleving' (RVS 2016). Ook de RVS heeft een signalerende taak over ontwikkelingen die vanuit ethische perspectief voor het volksgezondheidsbeleid van belang zijn.

---

<sup>72</sup> De RVZ is sinds 1 januari 2015 met de Raad voor Maatschappelijke Ontwikkeling (RMO) samengevoegd tot de Raad voor Volksgezondheid en Samenleving (RVS)

Binnen het parlement bleef echter de zorg bestaan dat in het ontstane netwerk van ethische commissies onvoldoende oog was voor nieuwe en bredere ethische vragen dan waar de toetsingscommissies via de wet en vastgestelde procedures op toetsen. Ook waren politici bezorgd dat de ethische toetsing los was komen te staan van zorgen in het publieke debat, en er niet voldoende ruimte was voor de politiek om zich over nieuwe ethische vragen uit te spreken. In 2004 zegde de regering daarom toe een tweejaarlijkse trendanalyse uit te voeren, die deze bredere vragen kon signaleren en zo mogelijk aanleiding kon geven om bestaande toetsingskaders aan te passen of te herzien (Kamerstukken II 2003-2004, 27428, nr. 45). Ook 'kan er dynamiek ontstaan tussen de samenleving en de instituten en kan de Kamer haar politieke rol invulling geven' (Kamerstukken II 2003-2004, 27428, nr. 45). Bestaande adviesorganen en commissies, zoals de Commissie Genetische Modificatie, Commissie Biotechnologie bij Dieren, Centrale Commissie Mensgebonden Onderzoek, de Gezondheidsraad en het Centre for Society and Genomics, hebben de afgelopen jaren in wisselende samenstelling de analyse opgesteld.

### **Pleidooi voor een nationale Raad voor Ethiek en Biotechnologie**

In de eerste helft van het decennium pleitte het CDA herhaaldelijk voor het instellen van een nationale Raad voor Ethiek en Biotechnologie. Net als Zwitserland en Noorwegen, kende en kent Nederland geen door de overheid ingestelde nationale ethiekraad. Landen als Duitsland, Frankrijk, België, Italië, Griekenland en Denemarken hebben wel zo'n raad. Volgens Tweede Kamerlid Ormel (CDA) kon men via bovengenoemde trendanalyse wel signalen opvangen vanuit de samenleving, maar schoot het instrument tekort bij het politiek agenderen van die signalen (De Vriend 2006). Een nationale Raad voor Ethiek en Biotechnologie zou daar wel een rol in kunnen spelen.

Eind 2006 organiseerde de toenmalige staatssecretaris van VROM Van Geel een conferentie om de meerwaarde van een dergelijke Raad te bespreken (De Vriend 2006). Ter voorbereiding van de conferentie schetste de COGEM een aantal voor- en nadelen van een nationale raad ten opzichte van een meer gespecialiseerde commissies op basis van Europees onderzoek (Zoeteman & Widdershoven 2007). Een nationale raad is gezaghebbend, goed herkenbaar voor het publiek en biedt de politiek een duidelijk aanspreekpunt. Nadelen zijn de grotere afstand tot de praktijk, en de mogelijke verenging van ethische kwesties tot medische kwesties. Ook leven er vragen over hoe de adviezen van een nationale raad kunnen worden vertaald naar wetgeving en verantwoordelijkheid (wie is bijvoorbeeld de verantwoordelijke bewindspersoon?) Tijdens de conferentie vonden vrijwel alle deelnemers dat er meer structurele aandacht nodig was voor ethische kwesties rondom biotechnologie, maar een meerderheid zag geen meerwaarde in een nationale raad (Verslag conferentie). Als gevolg werd een dergelijke nationale Raad voor Ethiek en Biotechnologie niet ingesteld (Kamerstukken II 2006-2007, 27428, nr. 85).

### **Aandacht voor risico's en maatschappelijke aspecten van nanotechnologie**

In de tweede helft van het decennium kwam er beleidsmatig aandacht voor nanotechnologie. In 2005 besloot de toenmalige regering een kabinetsvisie over nanotechnologieën uit te brengen. Een jaar later werd de visie 'Van klein naar groots' gepresenteerd. Een van de redenen voor een kabinetsbrede visie was dat er op dit technologiegebied zoveel gebeurde 'dat met het oog op samenhang in het beleid een gecoördineerde aanpak is vereist' (Kamerstukken II 2006-2007, 29338, nr. 54). De omgang met ethische en maatschappelijke vragen was één van de actielijnen uit de visie. Er moest een brede commissie komen om in een vroeg stadium ongewenste of

onschadelijke gevolgen van nanotechnologieën op het gebied van gezondheid, arbeidsomstandigheden, milieu, ethiek en sociale verhoudingen te identificeren.<sup>73</sup> Dit werd de Commissie Maatschappelijke Dialoog Nanotechnologie (CieMDN), die in 2009 van start ging.<sup>74</sup> In 2011 kwam de commissie met haar eindrapport 'Verantwoord verder met nanotechnologie'. Burgers vonden een adequaat systeem van onderzoek, vergunningverlening en toezicht noodzakelijk om nanotechnologieën op een verantwoorde manier toe te passen (Nanopodium 2011).

### **Behoeftte aan integratie van ethisch, juridisch en sociaal onderzoek**

Tijdens dit decennium groeide tevens de aandacht voor onderzoek naar ethische, juridische en maatschappelijke aspecten gekoppeld aan technologisch en wetenschappelijk onderzoek. Zo werd in 2004 het Center for Society and Genomics (CSG) opgericht.<sup>75</sup> De missie van het CSG was het begrijpen en verbeteren van de interactie tussen samenleving en genomics. Het CSG combineert sociaalwetenschappelijk, filosofisch en ethisch onderzoek met maatschappelijk interactie, dialoog en educatie. Ook binnen het NanoNed, het eerste nationale onderzoeksprogramma op het gebied van nanotechnologie, was er een specifiek technology assessment-onderzoeksprogramma (TA nanoNed). Daarnaast dwong de Tweede Kamer af dat binnen de opvolger van NanoNed, het omvangrijke NanoNextNL-programma (2010-2016), vijftien procent van het onderzoeksgeld besteed zou worden aan risk assessment & technology assessment (RATA).

Zowel op nationaal als op Europees niveau kreeg gelijktijdig onderzoek naar maatschappelijke en ethische vragen rondom technologie steeds meer aandacht in de agendering van onderzoek. In Nederland startte in 2008 bijvoorbeeld het 'Maatschappelijk Verantwoord Innoveren'-programma van NWO. Belangrijke eisen bij de toekenning zijn dat de projecten bijdragen aan beleidsdoelen (maatschappelijke uitdagingen) en dat de betrokkenheid van gebruikers is ingebouwd. Ook in Europa kwam er in onderzoeksprogramma's nadrukkelijker aandacht aan het concept 'Responsible Research Innovation' (zie onderzoeksprogramma's Horizon 2020 en Europe 2020) (Von Schomberg 2011; Owen et al. 2012). Centraal hierbij staat een open benadering waarin verschillende stakeholders in een vroeg stadium van onderzoek betrokken zijn om kennis op te doen over de consequenties van mogelijke innovaties, deze te evalueren in termen van maatschappelijke behoeften en normen en waarden, en deze vervolgens als leidraad te gebruiken bij alle fasen van het onderzoeksproces (EC 2013).

---

<sup>73</sup> Ze volgt daarmee een advies, 'Betekenis van nanotechnologieën voor de gezondheid', op van de Gezondheidsraad uit 2006.

<sup>74</sup> De commissie heeft als taak een publieke agenda (een prioriteitenlijst van te bespreken onderwerpen) te ontwikkelen en een maatschappelijke dialoog voor die onderwerpen te faciliteren, met een focus op maatschappelijke en ethische aspecten van nanotechnologie. Zie [wetten.overheid.nl/BWBR0025574/2009-04-01](http://wetten.overheid.nl/BWBR0025574/2009-04-01)

<sup>75</sup> Het Center for Genomics en Society is onderdeel van het Netherlands Genomics Initiative. Het initiatief startte in 2002 en was in de eerste fase gericht op de kennisinfrastructuur in Nederland (bundeling van onderzoeksgroepen, bedrijven en ziekenhuizen in centra). De tweede fase van 2008 was meer gericht op het omzetten van wetenschappelijke resultaten in concrete bijdragen aan maatschappelijk welzijn en economische groei.

## 4.6 Jaren 2010: behoefte aan reflectie op en debat over maatschappelijke en ethische aspecten van innovatie

In Nederland werden in 2014 twee moties ingediend en breed ondersteund die laten zien dat er in de Eerste Kamer vanuit politiek-bestuurlijk oogpunt behoefte bestaat aan meer (systematische) reflectie op de maatschappelijke en ethische betekenis van innovatie.

In maart 2014 verzocht senator Ester (ChristenUnie) de regering om structureel plaats in te ruimen in het technologie- en innovatiebeleid voor reflectie op ethische vragen en om het parlement daarover periodiek te informeren (Kamerstukken I 2013-2014, 33750, XIII). De motie verwijst hierbij naar convergerende technologieën als nanotechnologie, informatietechnologie, biotechnologie en cognitieve technologie (zogenoemde NBIC-convergentie). In reactie hierop stuurde de minister van Economische Zaken in mei 2016 een brief aan de Eerste Kamer met een overzicht van activiteiten binnen huidige innovatiebeleid waardoor de regering aandacht geeft aan maatschappelijke vragen. Het kabinet is voornemens om elk jaar een dergelijk overzicht in de Voortgangsrapportage Bedrijvenbeleid op te nemen. De Eerste Kamer heeft de minister verzocht niet alleen de activiteiten op een rij te zetten, maar ook aan te geven welke beleidsconsequenties daar mee samenhangen.

In september 2014 verzocht het Eerste Kamerlid Gerkens (SP) de regering het Rathenau Instituut te vragen een onderzoek te doen naar de wenselijkheid van een commissie die kan adviseren over de ethische kant van de digitalisering van de samenleving (Eerste Kamer 2014-2015, CVIII, E). De motie verwees hierbij naar de opkomst van het Internet of Things.

## 4.7 Noodzaak voor een breed perspectief op het governance-ecosysteem

### Motie Gerkens in historisch perspectief

Het historisch overzicht maakt duidelijk dat gedurende de gehele periode politieke en maatschappelijke aandacht geweest is voor diverse ethische en maatschappelijke aspecten van ICT. Sinds de volkstelling van 1971 is er aandacht voor privacyvraagstukken die samenhangen met ICT-ontwikkelingen. Dit leidde tot het opnemen van privacy als grondrecht in de gewijzigde grondwet van 1983 en tot wetgeving op het gebied van persoonsgegevens. Eind jaren zeventig ontstond de vrees dat micro-elektronica tot veel baanverlies zal leiden. De Commissie Rathenau kreeg de opdracht naar de maatschappelijke effecten van de opkomst van de micro-elektronica te kijken. In de tweede helft van de jaren negentig werd naar aanleiding van de opkomst van het internet de staatscommissie Franken ingesteld om vanuit digitalisering naar de grondwet te kijken. Infodrome werd opgericht om naar de rol van de overheid in de informatiesamenleving te kijken. In 2014 zetten de moties Ester (verwijzend naar NBIC-convergentie) en Gerkens (verwijzend naar de opkomst van het Internet of Things) digitalisering en de maatschappelijke en ethische kwesties die daardoor opkomen opnieuw op de politieke agenda. De ogen zijn niet langer enkel gericht op wetenschappelijk onderzoek, maar op het gehele proces van innovatie.

### Breed perspectief op het governance-ecosysteem

Concluderend leveren het historisch overzicht en de voorgaande hoofdstukken drie redenen om het governance-ecosysteem rondom digitalisering, ethiek en maatschappij breed te onderzoeken, overeenkomstig de achterliggende zorg van de motie Gerkens (zie hoofdstuk 1).

Ten eerste heeft digitalisering inderdaad invloed op allerlei wetenschappelijke, technologische en maatschappelijke ontwikkelingen, omdat ICT een *enabling technology* is (zie hoofdstuk 2).

Ten tweede toont de historie dat diverse typen commissies worden ingeschakeld om zich te buigen over de governance van ethische en maatschappelijke kwesties rondom technologie. We noemen hier vier soorten:

- Staatscommissies kunnen een rol spelen bij het voorbereiden van een grondwetswijziging of het onderzoeken of digitalisering wijziging van de grondwet vereist. Bijvoorbeeld de staatscommissie Cals/Donner (1967-1971), de staatscommissie Franken 'Grondrechten in het digitale tijdperk' (1999-2000) en de staatscommissie Thomassen (2009-2010).
- Adviescommissies wordt gevraagd om ethische en maatschappelijke aspecten van nieuwe ontwikkelingen in wetenschap en technologie in kaart te brengen en de regering daarover te adviseren. Een voorbeeld is de commissie Rathenau die zich eind jaren zeventig boog zich over de maatschappelijke gevolgen van micro-elektronica en de Brede DNA Commissie die tussen 1981 en 1983 de mogelijke toepassingen, maatschappelijke en ethische aspecten van recombinant-DNA-onderzoek in kaart bracht.
- Commissies die als taak hebben een publiek debat te organiseren, zoals de commissie Terlouw die het publieke debat 'Eten en genen' (2001) begeleidde of de Commissie Maatschappelijke Dialoog Nanotechnologie (CieMDN), die in 2009 een maatschappelijke dialoog over nanotechnologie organiseerde.
- Naast deze incidentele commissies zijn er meer permanente commissies op specifieke terreinen. Dit zijn bijvoorbeeld de Centrale Commissie Mensgebonden Onderzoek (CCMO) en diverse lokale medisch-ethische toetsingscommissies (METCs). De Commissie Genetische Modificatie (COGEM) heeft een signalerende taak op het gebied van de ethische aspecten verbonden aan de genetische modificatie van organismen.<sup>76</sup>

Dit houdt in dat we niet slechts naar een deelaspect van de omgang met ethische aspecten van de digitaliserende samenleving kunnen kijken, maar dat een breed palet van governance-activiteiten op het gebied van digitalisering, ethiek en maatschappij relevant is.

Ten derde sluit de motie Gerkens aan bij een parlementaire traditie om de toekomstbestendigheid van het bestaande governance-ecosysteem voor maatschappelijke en ethische aspecten van technologische ontwikkelingen te bevragen. Het parlement sprak de afgelopen decennia diverse malen over de adequaatheid van de politiek-bestuurlijke omgang met maatschappelijke en ethische kwesties rond wetenschap en technologie. Dit gebeurde vaak naar aanleiding van nieuwe doorbraken in de wetenschap of technologie.

---

<sup>76</sup> We zagen dat de ontwikkeling van DECs en METCs startte als een vorm van zelfregulering op decentraal niveau en over een lange periode via professionalisering (denk aan de oprichting van de Nederlandse Vereniging van Dierexperimentencommissies – NVDEC in 1995) en via wetgeving verankerd is. Bij die verankering en institutionalisering speelt wetgeving op Europees niveau een steeds grotere en op Europese schaal uniformerende rol.

Het opbouwen van een governance-ecosysteem kost vaak tientallen jaren. In de jaren zeventig en tachtig was de vraag om de maatschappelijke en ethische consequenties van technologische ontwikkelingen beter zichtbaar te maken. Dat leidde tot de institutionalisering van technology assessment en de oprichting van NOTA (later het Rathenau Instituut). Begin jaren negentig vroeg het parlement zich de ethische toetsingscommissies op het terrein van mensgebonden onderzoek (METCs) en dierexperimenten (DECs) nog wel op adequate wijze ethische en maatschappelijke aspecten meenamen in de besluitvorming. Dat leidde tot standaardisering, professionalisering en wettelijke verankering van METCs en DECs en duurde tientallen jaren. En ondanks de wettelijke verankering en de installering van nieuwe commissies, zoals de COGEM, stak begin deze eeuw de twijfel over de adequaatheid van het stelsel weer de kop op. Het parlement vroeg de regering of het ontstane netwerk van toetsingscommissies voldoende oog had voor nieuwe en bredere ethische vragen dan waar toetsingscommissies via wet en vastgestelde procedures op toetsen. Het parlement vroeg om reflectie op systeemniveau over het gehele stelsel van organisaties en commissies die zich bezig houden met de relatie maatschappij, ethiek en wetenschap en technologie. De behoefte aan samenhang uitte zich in de jaren 2000 bijvoorbeeld in de vraag om een integraal ethisch toetsingskader te ontwikkelen en in het pleidooi om een nationale Raad voor Ethiek en Biotechnologie in te stellen.

In de historische politieke discussies zien we drie aspecten periodiek terugkeren:

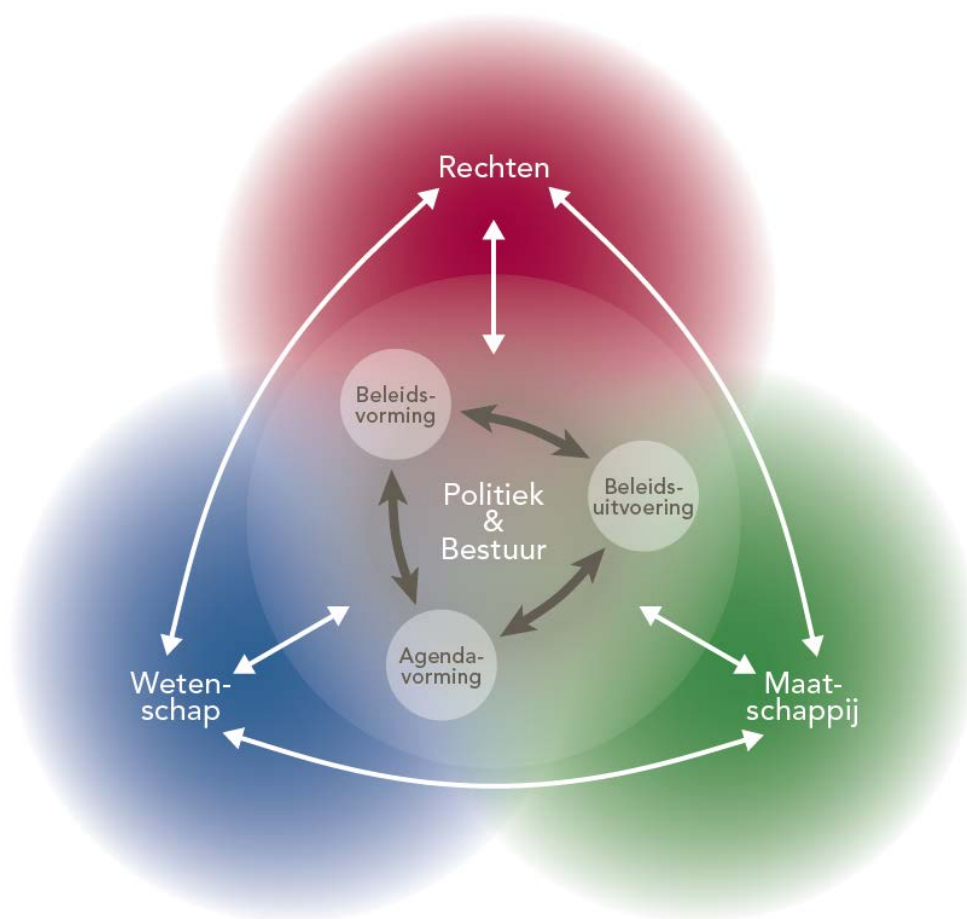
- Het belang van het systematisch verkennen van nieuwe ethische en maatschappelijke vragen rondom nieuwe technologie en het publieke én politieke debat daarover (waaruit bestaan de zorgen precies en welke waarden zijn in het geding?)
- De vraag of beleid voldoende inspeelt op gesignaleerde zorgen (met andere woorden, worden signalen wel vertaald naar regelgeving, sluit bestaande regelgeving aan bij nieuwe ontwikkelingen of is er nieuwe regelgeving nodig). En:
- De vraag of bestaande regelgeving en met name de uitvoering daarvan nog voldoende aansluit bij nieuwe ontwikkelingen en leidt tot maatschappelijk gewenste uitkomsten.

Er is dus een duidelijke Parlementaire traditie om met het oog op nieuwe wetenschappelijke en technologische ontwikkelingen de toekomstbestendigheid van het bestaande governance-ecosysteem te bevragen. De recente moties van Ester (2014) en Gerkens (2014) sluiten direct aan bij deze traditie. In dit geval zijn het de NBIC-convergentie en de opkomst van het Internet of Things die de meta-governancevraag doen rijzen of het huidige stelsel nog adequaat is en dat in de toekomst ook zal zijn. Om de analyse van het governance-ecosysteem aangaande de omgang met maatschappelijke en ethische aspecten op het gebied van digitalisering mogelijk te maken, ontwikkelen we in de volgende paragraaf op basis van het historische overzicht een conceptueel raamwerk voor dat ecosysteem.

## 4.8 Raamwerk voor het governance-ecosysteem

Op basis van het historisch overzicht onderscheiden we governance-activiteiten in vier domeinen, die op complexe wijze met elkaar interacteren (zie figuur 4.1): grond- en mensenrechten, maatschappij, wetenschap, en politiek en bestuur. Binnen de politiek-bestuurlijke sfeer onderscheiden we: a) agendavorming, b) beleidsvorming en -bepaling, en c) beleidsuitvoering. Bij beleidsvorming en -bepaling is er een speciale rol weggelegd voor het parlement. Hieronder lichten we toe op welke wijze deze vier domeinen een rol spelen binnen het governance-ecosysteem voor de omgang met maatschappelijke en ethische aspecten rond wetenschap en technologie. Aan het einde van deze paragraaf reflecteren we kort op de dynamiek van het governance-ecosysteem en het gegeven dat het opbouwen daarvan tientallen jaren kost.

**Figuur 4.1** Raamwerk voor het governance-ecosysteem



### 4.8.1 Mensenrechten, grondrechten en wet- en regelgeving

Het eerste domein van governance-activiteiten dat we beschrijven, richt zich op de rol van grond- en mensenrechten. In de historische schetsen zagen we dat ethische en maatschappelijke discussies rond nieuwe technologie vaak draaien om de vraag welke waarden in het geding zijn, waarbij vaak



wordt verwezen naar grond- en mensenrechten. Mensenrechten zijn rechten die ieder mens toekomen. Mensenrechten dienen mensen te beschermen tegen de macht van de staat en moeten ervoor zorgen dat iedereen kan leven in menselijke waardigheid.<sup>77</sup> Mensenrechten vormen vaak de basis voor wetgeving en overheidsbeleid. Ze zijn met name vastgelegd in de Universele Verklaring van de Rechten van de Mens van de Verenigde Naties (1948), het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) van de Raad van Europa (1950, en sinds 1998 bindend voor alle lidstaten van de Raad van Europa), en het Handvest van de grondrechten van de Europese Unie (2000). Mensenrechten worden ook vastgelegd in nationale grondwetten, zoals de Nederlandse Grondwet. Daarin worden ze vaak 'grondrechten' genoemd. Deze verdragen verankeren voor Nederland belangrijke waarden zoals menselijke waardigheid, vrijheid, veiligheid, gelijkheid en rechtvaardigheid. Technologische ontwikkelingen kunnen de rechten van mensen versterken, maar deze tevens onder druk zetten, of nopen tot de formulering van nieuwe mensen- of grondrechten. De historische schets liet diverse voorbeelden daarvan zien. Denk aan privacy dat in 1983 als een nieuw grondrecht (artikel 10) aan de Grondwet werd toegevoegd (zie kader 4.5). De opkomst van het internet in 1999 leidde tot de instelling van de commissie Franken, de staatscommissie 'Grondrechten in het digitale tijdperk'. Voor biotechnologie stelden de Raad van Europa en UNESCO enkele specifieke verdragen op, zoals in 1997 het Verdrag van Oviedo en de Universal Declaration on the Human Genome and Human Rights, en later de International Declaration on Human Genetic Data (2003) en de Universal Declaration on Bioethics and Human Rights (2005) (zie ook kader 4.2).

#### **Kader 4.5 Privacy en onaantastbaarheid van het lichaam als Nederlandse grondrechten**

##### **Artikel 10: Privacy**

Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.

De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.

De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

##### **Artikel 11: Onaantastbaarheid van het lichaam**

Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op onaantastbaarheid van zijn lichaam.

In de praktijk zijn deze algemene kaders vaak onvoldoende om specifieke kwesties die spelen rond een bepaalde technologie of praktijktoepassing het hoofd te kunnen bieden. Deze aspecten worden daarom vaak geregeld in specifieke wetten en regelgevende kaders. Met betrekking tot het

<sup>77</sup> Zie website van het College voor de Rechten van de Mens: [mensenrechten.nl/wat-zijn-mensenrechten/wat-zijn-mensenrechten](https://mensenrechten.nl/wat-zijn-mensenrechten/wat-zijn-mensenrechten)

grondrecht op privacy regelt de Wet bescherming persoonsgegevens (Wbp) bijvoorbeeld in meer detail de manier waarop persoonsgegevens verwerkt mogen worden. Een ander voorbeeld is de Wet medisch-wetenschappelijk onderzoek met mensen (Wmo, 1998). Deze wet geeft een nadere invulling van het grondrecht op onaantastbaarheid van het lichaam (zie kader 4.5).

## 4.8.2 Maatschappelijke actoren en debat

De volgende governance-activiteit uit het raamwerk richt zich op de rol van diverse maatschappelijke actoren en maatschappelijk debat. Het kan in de praktijk, om uiteenlopende redenen, lastig zijn om de omgang met maatschappelijk-ethische kwesties wettelijk vast te leggen, terwijl er binnen bedrijven of sectoren wel een behoefte kan bestaan om zaken vast te leggen. Gedragscodes, zoals maatschappelijk verantwoord ondernemen ten aanzien van mensenrechten (zie kader 4.6), en zelfregulering zijn een manier om invulling te geven aan die behoefte. Daarnaast is duidelijk dat er in de Nederlandse samenleving altijd verschillen in opvattingen en levensovertuigingen zullen bestaan en dat ieder individu, organisatie of bedrijf ook zelf keuzes maakt over welke toepassingen van nieuwe technologie zij wel of niet wenselijk achten.

### **Kader 4.6 United Nations Guiding Principles on Business and Human Rights**

In juni 2011 zijn de *United Nations Guiding Principles on Business and Human Rights* (UNGP's) aangenomen. De UNGPs zijn ontwikkeld onder leiding van VN-Speciaal Vertegenwoordiger Ruggie (daarom ook wel Ruggie principles genoemd). De principes bestaan uit drie pijlers. De eerste pijler herbevestigt de plicht van staten om mensenrechten te beschermen. De tweede pijler is gericht op de verantwoordelijkheid van bedrijven om mensenrechten te respecteren. De derde pijler betreft de noodzaak om slachtoffers van mensenrechtenschendingen door activiteiten van bedrijven mogelijkheden te geven op herstel en/of genoegdoening (Kamerstukken II 2015-2016, 26485, nr. 219). De UNGPs leggen geen juridische verplichtingen op maar vormen een gezaghebbende internationale standaard. De verantwoordelijkheid van bedrijven om mensenrechten te respecteren is in de Richtlijnen voor Multinationale Ondernemingen van de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO-richtlijnen) opgenomen.<sup>78</sup> Bedrijven dienen zich actief in te spannen om risico's op schendingen van mensenrechten door henzelf of partijen in hun keten te onderkennen en waar mogelijk schendingen te voorkomen.

Politieke discussies over ethische en maatschappelijke vragen rond nieuwe technologie spelen zich vaak af op het grensvlak van algemene waarden en vastgelegde verantwoordelijkheden van overheden enerzijds (zoals het beschermen van de volksgezondheid, of de persoonlijke levenssfeer van burgers) en het ruimte geven aan individuele afwegingen en keuzes van individuen, organisaties en bedrijven anderzijds. In het algemeen geldt dat de Nederlandse overheid deze beslissingen op het laagst mogelijk niveau zal willen leggen (het subsidiariteitsbeginsel).

<sup>78</sup> De OESO Principes voor Multinationals (OESO 1976; 2011) gaan over over bedrijfsethische kwesties en verantwoordelijke bedrijfscodes. De Nederlandse overheid heeft deze richtlijnen onderschreven; zij verwacht van bedrijven dat ze maatschappelijk verantwoord ondernemen (TK 2012-2013).

Tegelijkertijd vraagt de vrijheid om individueel ethische keuzes te *kunnen* maken in de praktijk ook om maatschappelijke keuzes. Denk bijvoorbeeld aan euthanasie of het kunnen plegen van abortus. In Nederland kunnen individuen, onder bepaalde voorwaarden, deze keuze maken, maar wordt die keuze mogelijk door het organiseren van een maatschappelijke en wettelijke praktijk daar om heen.

Het politieke en maatschappelijke debat kunnen elkaar voeden. De historische schets liet zien dat de overheid met regelmaat het publieke debat over de ethische en maatschappelijke aspecten van nieuwe technologie wilde stimuleren, zoals via de vanuit de overheid geïnitieerde debatten over genetisch gemodificeerd voedsel of nanotechnologie. Het Rathenau Instituut heeft onder meer de taak om het publieke en politieke debat over de ethische en maatschappelijke kanten van technologie te stimuleren.

### **4.8.3 Wetenschappelijke kennis**

Als derde domein van governance-activiteiten bespreken we de rol van wetenschappelijke kennis binnen het governance-ecosysteem. Deze rol is divers en speelt op vele niveaus.

Wetenschappelijke kennis kan behulpzaam zijn bij zowel de signalering als articulatie van maatschappelijke en ethische aspecten (agendavorming), bij het formuleren van een beleidsopvatting en bepalen van een handelingsperspectief (beleidsvorming) en bij reflectie op de uitvoering van beleid. Ethische reflectie (Ladikas et al. 2015) of ethische analyse en fundering (Kamerstukken II 1990-1991, 21319, nr. 12) is ook een vorm van wetenschappelijke kennis die relevant is in het governance-ecosysteem. Daarmee wordt het diepere denken over ethiek en achterliggende normen bedoeld, zoals dat veelal door ethici en filosofen op universiteiten wordt uitgevoerd. Wetenschappelijke kennis voor beleid wordt door een netwerk van adviesraden en publieke kennisorganisaties aangeleverd.

Het historische overzicht liet zien dat tijdens het eerste decennium van deze eeuw de aandacht en financiering groeiden voor onderzoek naar de integratie van kennis over ethische, juridische en maatschappelijke aspecten van technologie en wetenschap met de technologische ontwikkelingen. Dit uitte zich bijvoorbeeld in de oprichting van het Center for Society and Genomics (CSG) als onderdeel van het Netherlands Genomics Initiative of het risk assessment en technology assessment (RATA) onderzoeksprogramma als onderdeel van het nationale nanotechnologie-onderzoeksprogramma NanoNextNL.

### **4.8.4 Politiek en bestuur**

Het vierde domein van het raamwerk gaat in op de rol van politiek en bestuur binnen het governance-ecosysteem. We maken een globaal onderscheid tussen drie processen in het beleid waarin ethische en maatschappelijke vragen over technologie een rol spelen: de agendavorming, beleidsvorming en -bepaling, en de beleidsuitvoering. We bespreken deze drie fases hieronder in

meer detail hieronder. Ter illustratie beschrijven we steeds een aantal organisaties die op het terrein van de bio-ethiek een rol spelen.<sup>79</sup>

## Agendavorming

Bij agendavorming spelen het signaleren, articuleren en agenderen van ethische en maatschappelijke vragen over nieuwe ontwikkelingen in de wetenschap en technologie een belangrijke rol. Hierbij zijn professionele adviesorganen betrokken, die als taak hebben nieuwe maatschappelijke en ethische vragen te signaleren, te agenderen, en beleidsmakers en politici daarover te adviseren. Daarnaast spelen maatschappelijke organisaties, publieke percepties, burgers en de media een rol. Deze fase wordt ook wel 'ethische deliberatie' genoemd (Ladikas et al. 2015). Minister Ritzen sprak in dit kader van de signalerings- en articulatiefunctie (Kamerstukken II 1990-1991, 21319, nr. 12). Belangrijk in deze fase is dat verschillende opvattingen, argumenten en belangen zo breed mogelijk zijn vertegenwoordigd. Hierbij staan democratische waarden en de kwaliteit van de uitwisseling van visies en belangen centraal.

Tijdens deze voorbereidende fase kan een *aggregatieproces* tot stand komen (Stemerding & Kater 2005; Van der Meulen & Rip 1998), waarin 'intermediaire instanties' (instanties tussen beleid, wetenschap en burgers) visies en zorgen over nieuwe technologieën verwoorden, duiden en bij de politiek onder de aandacht brengen. Signalen over mogelijke ethische en maatschappelijke kwesties over nieuwe ontwikkelingen in wetenschap en technologie vertalen zij naar de huidige beleidscontext en worden op de beleidsagenda gezet.

Op het terrein van de bio-ethische en biomedische kwesties spelen bijvoorbeeld de Gezondheidsraad (opgericht in 1902) en de Raad voor de Volksgezondheid en Samenleving (RVS) een officiële rol in deze fase. De Gezondheidsraad en de RVS geven invulling aan hun signalerende taak via het in 2003 ingestelde Centrum voor Ethiek en Gezondheid (CEG). De Commissie Genetische Modificatie (COGEM) adviseert de regering over mogelijke risico's van productie en handelingen met genetisch gemodificeerde organismen (ggo's) voor mens en milieu.

## Beleidsvorming en -bepaling

Deliberatie kan leiden tot beleidsvorming en -bepaling: een fase waarin (politieke) besluiten worden voorbereid en genomen over de gesignaleerde maatschappelijke en ethische vragen. Om dit mogelijk te maken, moet duidelijk gemaakt worden *wie* besluiten kan nemen, bijvoorbeeld een toezichthouder of toetsingscommissie (dit noemde Ritzen de 'gezaghebbende toedeling van waarden'). Bovendien moet duidelijk worden waarover besluiten moeten worden genomen, bijvoorbeeld dat er nieuwe regelgeving nodig is. In een democratische samenleving zijn er altijd verschillen van inzicht, mening en levensovertuiging over hoe om te gaan met maatschappelijk-ethische vragen. Daarom is de politieke besluitvorming door het parlement van belang. De fase van beleidsvorming en -bepaling kan leiden tot het opstellen of aanpassen van regelgevende kaders en tot beslissingen over andere beleidsinstrumenten, zoals het instellen van een trendanalyse, het

---

<sup>79</sup> We danken Boukje van der Zee voor het opstellen van een overzicht van relevante organisaties en instanties op dit vlak. Zie voor een uitgebreid overzicht van de historie en individuele beschrijving van betrokken raden en instanties Zoeteman & Widdershoven-Heerding (2007) en Rerimassie & Brom (2012).

instellen van een tijdelijke commissie, opzetten van een maatschappelijke dialoog, besluiten tot voorlichtingscampagnes, en het verstrekken van onderzoekfinanciering.

Op het terrein van de bio-ethiek en de biomedische kwesties zijn diverse ministeries betrokken bij het opstellen van beleid en bijbehorende regulerende kaders, zoals het Ministerie van Volksgezondheid, Welzijn en Sport (VWS), Ministerie van Economische Zaken en het Ministerie van Infrastructuur en Milieu. Sommige ministeries, zoals VWS, hebben een ethiekafdeling die zich bezig houdt met ethische kwesties. Het parlement speelt een aanjagende en controlerende rol en wijst regelmatig op de noodzaak voor een maatschappelijke dialoog rond een bepaalde technologie, of het aanscherpen van bestaande kaders.

### **Beleidsuitvoering**

Een derde fase bestaat uit de beleidsuitvoering waarin bovengenoemde beslissingen in de praktijk worden geïmplementeerd en uitgevoerd. Ook hierbij zijn allerlei intermediaire instanties betrokken die richting geven aan het vastgestelde beleid of dit uitvoeren. Denk aan toezichthouders die regelgevende kaders handhaven, de rechtelijke macht, of ethische toetsingscommissies die op basis van regelgevende kaders en protocollen keer op keer toetsen of partijen zich aan deze kaders gehouden hebben.

Op het terrein van de bio-ethiek en de biomedische kwesties hebben we in het historisch overzicht gesproken over de dierexperimentcommissies (DECs), de Centrale Commissie Dierproeven (CCD) en het Nationaal Comité advies dierproevenbeleid (NCad). Op het terrein van mensgebonden onderzoek spelen decentrale, erkende medisch-ethische toetsingscommissies (METCs), die vaak zijn verbonden aan een ziekenhuis, een rol. De Centrale Commissie Mensgebonden Onderzoek (CCMO) houdt toezicht op de werkzaamheden van de METCs en toetst in sommige situaties zelf.

## **4.9 Tot slot: Langetermijndynamiek van het governance-ecosysteem**

Op basis van het voorgaande kunnen we concluderen dat de bestuurlijke omgang met ethische en maatschappelijke kwesties rond wetenschap en technologie een lange adem vergen. Dat komt ten eerste omdat het lang kan duren voordat wetenschappelijke vindingen en technologische ontwikkelingen op brede schaal hun toepassing in de maatschappij vinden. Na de ontdekking van de recombinant-DNA-technologie midden jaren zeventig was er aanvankelijk bijvoorbeeld in een kleine kring van experts aandacht voor risico's en ethische kwesties die worden opgeroepen door gentechnologie. Het debat daarover richtte zich name op de modificatie van micro-organismen binnen gesloten systemen (die niet in het milieu komen). Het duurde tot de jaren negentig voordat mogelijke toepassingen op het terrein van planten, dieren en mensen in de media aandacht kregen. Dat zorgde voor een verbreding van het debat richting maatschappij en politiek. Die zichtbaarheid lijkt nodig om het debat te verbreden en voor politieke urgentie.

Een tweede reden waarom de opbouw van een governance-ecosysteem lang kan duren, is omdat de ontwikkeling van nieuwe grondrechten, nieuwe wetgeving, en de professionele opbouw van een toetsingssysteem vaak tientallen jaren in beslag neemt. De casus van de dierexperimenten illustreert dat mooi; het heeft twintig jaar geduurd sinds de eerste dierexperimentcommissies hun

beslag kregen om een het systeem te professionaliseren en uiteindelijk wettelijk te verankeren met de wijziging van de Wod in 1996, waarin de intrinsieke waarde van het dier centraal staat. Hetzelfde zien we bij mensgebonden onderzoek. Daar werden de eerste lokale medisch-ethische toetsingscommissies in de jaren zeventig ingesteld. Het duurde echter tot 1998 voordat deze praktijk wettelijk was geregeld.

Juist de combinatie van de twee dynamieken – zichtbaar en het publiek bespreekbaar worden van nieuwe ontwikkelingen en de borging van publieke waarden – kan problematisch zijn. Dat betekent namelijk dat het lang kan duren voordat ontwikkelingen in de wetenschap en technologie op de maatschappelijke en politieke agenda komen en het vervolgens opnieuw lang duurt voordat er een governance-ecosysteem voor de omgang met ethische en maatschappelijke kwesties is. In het volgende hoofdstuk onderzoeken we hoe het governance-ecosysteem op het gebied van de ethiek van digitalisering in Nederland functioneert.

# 5 Blinde vlekken in het governancelandschap

## 5.1 Inleiding

In hoofdstuk 3 hebben we een inventarisatie gemaakt van de belangrijkste ethische en maatschappelijke vraagstukken die digitalisering oproept.<sup>80</sup> In dit hoofdstuk kijken we hoe er met deze vraagstukken in het huidige governancelandschap wordt omgegaan, en op welke plaatsen zich blinde vlekken bevinden. Dat doen we aan de hand van het governanceraamwerk opgesteld in hoofdstuk 4 (zie figuur 4.1). We kijken net als in het vorige hoofdstuk, naar governance en meta-governance vragen: met andere woorden, welke vraagstukken worden gesignaleerd en geagendeerd; en door wie worden deze vraagstukken gesignaleerd en welke rollen spelen deze actoren in het governance-ecosysteem? Dat maakt duidelijk op welke posities én op welke thema's blinde vlekken zitten in het governance-ecosysteem. Met deze analyse kunnen we in het volgende hoofdstuk een antwoord geven op de vraag van de motie Gerkens naar de wenselijkheid van een commissie die kan adviseren over de ethische kant van de digitalisering van de samenleving.

De opbouw van dit hoofdstuk volgt de structuur van het raamwerk uit hoofdstuk 4. We beschrijven allereerst de drie domeinen wetenschap, grond- en mensenrechten en maatschappij. Vervolgens zoomen we in op het politiek-bestuurlijke domein, waarin we de processen van agendavorming, beleidsvorming en -bepaling, en beleidsuitvoering beschrijven:

- rol van de wetenschap (paragraaf 5.2);
- rol van grond- en mensenrechten (paragraaf 5.3);
- rol van maatschappelijke actoren (paragraaf 5.4);
- rol van politiek en bestuur;
  - a. agendavorming (paragraaf 5.5);
  - b. beleidsvorming en -bepaling (paragraaf 5.6);
  - c. beleidsuitvoering (paragraaf 5.7);
- conclusies (paragraaf 5.8).

### Reikwijdte van de analyse

Dit hoofdstuk beschrijft alleen initiatieven met betrekking tot digitalisering én maatschappelijke en ethische vragen. Onze analyse richt zich op Nederland, maar benoemt ook enkele interessante buitenlandse ontwikkelingen. We hebben daarbij gekeken naar ontwikkelingen tot oktober 2016. In de diverse paragrafen bespreken we de activiteiten van diverse organisaties. Dat doen we aan de hand van hun institutionele positie. Zo worden de acties van ministeries in paragraaf 5.6 'Beleidsvorming' besproken en die van de Autoriteit Persoonsgegevens (AP) in paragraaf 5.7 over

---

<sup>80</sup> We beschreven vraagstukken zoals de bescherming van privacy van gevoelens bij emotieherkenningstechnologie, discriminatie door algoritmen die rechters adviseren, en digitale veiligheid bij aan het internet verbonden pacemakers die gehackt kunnen worden. We kwamen tot zeven belangrijke thema's: privacy, autonomie, veiligheid, controle over technologie, menselijke waardigheid, rechtvaardigheid en machtsverhoudingen.

‘Beleidsuitvoering’. Vanzelfsprekend kunnen organisaties ook acties buiten hun eigen domein ondernemen – bijvoorbeeld acties van een ministerie om een maatschappelijke dialoog te stimuleren – deze acties beschrijven we dan vanuit de institutionele positie van de actor. Dit hoofdstuk biedt een beknopt overzicht van de activiteiten die diverse organisaties en actoren voorstellen, voorbereiden, initiëren of uitvoeren om in te spelen op maatschappelijke en ethische kwesties die verband houden met de digitalisering van de samenleving. We sluiten elke paragraaf af met een tabel waarin de meest relevante initiatieven per domein zijn samengevat. Een uitgebreidere beschrijving van de betreffende organisaties en hun activiteiten is te vinden in appendix A.

## 5.2 Rol van de wetenschap

In deze paragraaf beschrijven we de rol die wetenschap in het governance-ecosysteem inneemt bij het signaleren en het articuleren van de ethische vraagstukken die digitalisering oproept.

### In politiek en bestuur

Met kennis en reflectie op technologische ontwikkelingen – waarin sociale- en geesteswetenschappen een belangrijke rol spelen – voedt de wetenschap de maatschappelijke en politiek-bestuurlijke discussie. De wetenschap draagt direct bij het politiek-bestuurlijke proces door in opdracht wetenschappelijke kennis te leveren om politici en beleidsmakers te ondersteunen. Dit gebeurt bijvoorbeeld in de vorm van studies, of wanneer individuele wetenschappers als experts worden geraadpleegd tijdens een hoorzitting of rondetafelgesprek in de Tweede Kamer. In onze analyse in Appendix A zien we dat de wetenschap vaak een belangrijke rol speelt in de articulatie van concepten. De dissertatie Hofman uit 1995 leidde tot een discussie over het begrip ‘vertrouwelijke communicatie’ die uitmondde in het instellen van de staatscommissie Franken (Kamerstukken II 1996-1997, 25 443, nr. 1/2). Ook de betekenis van het concept privacy wordt in sterke mate gevoed door een wetenschappelijke discussie over het begrip (zie bijvoorbeeld Solove 2002). In dit kader is ook het onderzoeksproject van Prof. dr. B.J. Koops naar digitaal huisrecht als nieuw privacyconcept illustratief (Martijn 2016).

### In het maatschappelijk debat

Via de media dragen wetenschappers ook bij aan de maatschappelijke discussie. De wetenschapper Hawking waarschuwde samen met andere wetenschappers in de Britse krant *The Guardian* voor de existentiële gevaren van artificiële intelligentie (Hawking et al. 2014). Of de studie van Frey en Osborne (2013) die met berekeningen over de automatisering van bepaalde banen het startpunt vormde voor een discussie over de relatie tussen technologie en arbeid. Ook in Nederland speelt de wetenschap een belangrijke rol in het aanwakken van het maatschappelijke en het politieke debat. Hoogleraar filosofie Verbeek deed dat bijvoorbeeld met een opiniestuk waarin hij zich afvroeg hoe ver bedrijven mogen gaan met het inzetten van persuasieve technologie bij werknemers (Verbeek 2016). En het werk van de onderzoeksgroep van hoogleraar computerbeveiliging B. Jacobs (Radboud Universiteit 2016) leidde tot discussies en Kamervragen over digitale veiligheid.

### Bij maatschappelijk verantwoorde innovatie

Behalve het leveren van kennis zorgt de wetenschap ook voor innovaties die een antwoord kunnen geven op maatschappelijke en ethische kwesties, bijvoorbeeld oplossingen op het gebied van



privacy by design, of nieuwe cryptografische technieken die het internet veiliger kunnen maken. In onderzoeksfinanciering wordt er vanuit concepten zoals *Responsible Research and Innovation* en *Maatschappelijk Verantwoord Innoveren* (MVI) gedacht over de maatschappelijke meerwaarde van innovatie. Een belangrijk onderdeel van deze filosofie is dat ethische aspecten van innovatie in een vroeg stadium worden geïdentificeerd, en zo kunnen worden meegenomen in een ethische verantwoorde ontwikkeling van wetenschap en innovatie. In de wetenschapsvisie (Kamerstukken II, 2014-2015, 29338, nr. 141) en in de Kamerbrief over ethische aspecten van het innovatiebeleid (Kamerstukken I, 2015-2016, 33009 nr. 16) wordt het MVI-programma van NWO gezien als een belangrijke manier om al in de onderzoeksfase met de ethische en maatschappelijke vragen omtrent innovatie om te gaan. Daarnaast kijkt de wetenschap ook of zij zelf in het wetenschappelijk onderzoek op een verantwoorde manier met groeiende dataverzamelingen omgaat. De Koninklijke Nederlandse Academie van Wetenschappen (KNAW) raadt aan om een *Ethical Review Board Informatics* in te stellen om te beoordelen of er bij informaticaonderzoek op een verantwoorde manier met persoonlijke gegevens om wordt gegaan.

### **Conclusie**

Het domein van de wetenschap zorgt in het hele governance-ecosysteem voor reflectie en kennis over de ethische en maatschappelijke aspecten van digitalisering. Ze heeft daarmee invloed op het domein van politiek en bestuur, de maatschappij, en het domein van de grondrechten. De vragen die door de wetenschap worden gesignaleerd – beschreven in hoofdstuk 3 – vormen een belangrijke basis voor de adviesorganen en onderzoeksinstituten die zich bezig houden met het agendavorming in het politiek-bestuurlijke proces. Bovendien heeft zoals we zagen wetenschap ook direct invloed op het politieke en maatschappelijke debat en draagt zij ook daarin bij aan het agenderen van ethische en maatschappelijke kwesties van digitalisering.

## **5.3 Rol van grond- en mensenrechten**

Grond- en mensenrechten vormen de basis waarin maatschappelijke waarden en fundamentele vrijheden zijn vastgelegd. Deze rechten zijn vastgelegd in de Nederlandse Grondwet, het EU-Handvest van de Grondrechten en door Nederland geratificeerde internationale verdragen, zoals de Universele Verklaring van de Rechten van de Mens van de Verenigde Naties (1948). Ze verankeren belangrijke waarden zoals menselijke waardigheid, vrijheid, veiligheid, gelijkheid en rechtvaardigheid. In hoofdstuk 3 zagen we dat digitalisering vele fundamentele menselijke waarden en rechten kan aantasten. Daarmee leidt digitalisering tot discussies over bescherming van mensenrechten in het digitale tijdperk. Dat roept de vraag op welke ontwikkelingen er in Nederland zijn op het gebied van de grondrechten en of daarin ook nieuwe ethische en maatschappelijke vragen zijn belegd.

### **Nederland**

In de discussie over grondrechten en digitalisering in Nederland is de opkomst van het internet in de afgelopen jaren een belangrijke drijvende kracht geweest. Twee staatscommissies hebben zich uitgesproken over de vraag of Nederlandse Grondwet nog adequaat is in het digitale tijdperk; de Commissie Franken en de Commissie Thomassen. Beide commissies richten zich op de grondwetsartikelen 7 (vrijheid van meningsuiting), 10 (eerbiediging van de persoonlijke levenssfeer) en 13 (vertrouwelijke communicatie). Beide commissies zochten naar een technologie-neutrale

invulling van deze grondrechten om op die manier de Grondwet toekomstbestendig te maken. Op dit moment loopt de procedure voor aanpassing van Grondwetsartikel 13. Er is ook een langlopende discussie over artikel 120 (verbod op constitutionele toetsing).<sup>81</sup> Opheffing van dat grondwetsartikel zou burgers en maatschappelijke organisaties meer mogelijkheden bieden om diverse wetten aan de Grondwet te toetsen, bijvoorbeeld als deze de privacy aantasten.

## Europa

Op Europees niveau zijn met name de Bioethische Commissie (DH-BIO) en de Parlementaire Assemblée (PACE) van de Raad van Europa actief op de relatie tussen digitalisering en fundamentele rechten. Binnen DH-BIO en PACE leeft sterk het besef dat op dit moment een brede waaier van opkomende technologieën tal van ethische kwesties met zich meebrengt, die allerlei consequenties kunnen hebben voor mensenrechten. Technologische convergentie zorgt ervoor dat de gebruikelijke scheidslijnen binnen het ethische debat en tussen de kaders die we gebruiken om met ethische kwesties en mensenrechten om te gaan niet langer vanzelfsprekend zijn. PACE gaat onderzoeken op welke wijze convergerende technologieën, artificiële intelligentie en robotica ethische kwesties oproepen en diverse mensenrechten uitdagen. Daarbij wordt de vraag gesteld of het wenselijk is om een verdrag op te stellen dat specifiek ingaat op de bescherming van mensenrechten in relatie tot digitalisering, parallel aan de wijze waarop het Verdrag van Oviedo<sup>82</sup> dat doet voor biotechnologie (Van Est en Gerritsen nog te verschijnen).<sup>83</sup> Aangezien de Raad van Europa zich voorheen met name heeft beziggehouden met ontwikkelingen op het gebied van biotechnologie en de relatie informatietechnologie en privacy, verbreedt de Raad van Europa met haar interesse voor convergerende technologieën, robotica en artificiële intelligentie haar perspectief op technologie en mensenrechten sterk.

## Internationaal

Op mondiaal niveau houdt de Mensenrechtenraad van de Verenigde Naties zich bezig met de bescherming van de mensenrechten in de digitale wereld. Via de zogenaamde Internet Resolutie uit 2012 wordt herbevestigd dat internationale mensenrechtenverdragen ook gelden voor de digitale wereld. Deze verdragen zijn aldus technologie-neutraal verklaard. De Internet Resolutie waarborgt niet dat de mensenrechten in de digitale wereld ook daadwerkelijk ongeschonden blijven. De Mensenrechtenraad van de VN richt haar pijlen specifiek op privacy, mede in het licht van de toenemende surveillance, en de vrijheid van meningsvorming en -uiting. In 2015 stelde de VN een speciaal gezant voor privacy aan met als taak het verzamelen van informatie en het opstellen van aanbevelingen ter promotie van het recht op privacy (VN-resolutie 28/16). Binnen de UNESCO bereiden het IBC (International Bioethics Committee) en COMEST (World Commission on the Ethics of Scientific Knowledge and Technology) rapporten voor op het gebied van respectievelijk de ethiek van big data & health en van robotica.

---

<sup>81</sup> Constitutionele toetsing door de rechter houdt in dat de rechter toetst (of mag toetsen) of wetten al dan niet in overeenstemming zijn met de Grondwet. Deze discussie kent twee kampen. Voorstanders van constitutionele toetsing pleiten voor afschaffing van het toetsingsverbod (artikel 120), tegenstanders pleiten juist voor een artikel dat ook toetsing aan internationale verdragen onmogelijk maakt.

<sup>82</sup> Het Verdrag van Oviedo werd opgesteld op initiatief van de Raad van Europa en werd in 1997 opengesteld voor ondertekening. Het verdrag baseert zich op het Europees Verdrag voor de Rechten van de Mens en geeft invulling aan de bescherming van onder andere menselijke waardigheid in relatie tot de biogeneeskunde.

<sup>83</sup> Technological convergence, artificial intelligence and human rights. Motion for a resolution. Doc. 13833, 24 June 2015. Parliamentary Assembly of the Council of Europe. Zie [assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21951&lang=en](http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21951&lang=en)

## Conclusie

Naar aanleiding van de opkomst van het internet is er in Nederland sinds het midden van de jaren negentig aandacht voor de betekenis daarvan voor diverse grondrechten, met name privacy (art. 10), vertrouwelijke communicatie (art. 13) en vrijheid van meningsuiting (art. 7). De centrale zorg is dat nieuwe technologieën grondrechten onder druk kunnen zetten. De vraag of grondrechten in het licht van technologische ontwikkelingen nog adequaat zijn beschermd, keert daarbij telkens terug. Op dit moment loopt het proces voor aanpassing van grondwetsartikel 13. Maar er is slechts geringe aandacht voor de impact van het Internet of Things, robotica en AI op de grondrechten en een mogelijke behoefte aan nieuwe grondrechten die wordt opgeroepen door deze nieuwe digitaliseringsgolf. Op internationaal niveau wordt zichtbaar dat de bestuurlijke aandacht daarvoor de laatste jaren flink groeit, zoals ook tabel 5.1 laat zien.

**Tabel 5.1** Activiteiten binnen het domein van grond- en mensenrechten.

Wie/wat	Technologie	Issue	Actie
Staatscommissie Thomassen	Digitalisering	Specifiek: vrijheid van meningsuiting, privacy, vertrouwelijke communicatie	Voorstel tot grondwetswijziging art. 7, 10, 13
Regering	Digitalisering	Specifiek: vertrouwelijke communicatie	Grondwetswijziging art. 13
VN Mensenrechtenraad	Internet	Breed: mensenrechten op het Internet	Internetresolutie L13
VN Mensenrechtenraad	Internet	Specifiek: recht op vrijheid van mening en meningsuiting	Speciale gezant vrijheid van meningsuiting
VN Mensenrechtenraad	Digitalisering	Specifiek: recht op privacy	Speciale gezant privacy
UNESCO, IBC	Big data & health	Breed: ethische kwesties	Vorbereiding rapport
UNESCO, COMEST	Robotica	Breed: ethiek van robotisering	Vorbereiding rapport
Parlementaire Assemblee van de Raad van Europa (PACE) motie	NBIC-convergentie en artificiële intelligentie; digitalisering	Breed: impact NBIC op mensenrechten	Onderzoek behoefte verbreding werkveld van bio-ethiek naar NBIC-ethiek
Toetsing aan grondrechten en mensenrechtenverdragen	Specifiek case by case	Specifiek case by case	NGO's en individuen kunnen zich beroepen op grondrechten

## 5.4 Rol van maatschappelijke actoren

Maatschappelijke actoren spelen een belangrijke rol in de governance van maatschappelijke en ethische vragen omtrent digitalisering. Burgers, bedrijven en maatschappelijke organisaties geven met hun acties vorm aan de manier waarop digitale technologie een plek krijgt in de maatschappij. We kijken hier naar de acties die zij nemen om met ethische vraagstukken van digitalisering om te gaan.

### Politieke en maatschappelijke discussies

Diverse maatschappelijke organisaties spelen een belangrijke rol in het maatschappelijk en politieke debat over digitalisering. De voornaamste aandacht gaat daarin uit naar privacy en digitale veiligheid. Voorbeelden zijn de Big Brother Awards van Bits of Freedom die tot Kamervragen leidden (Handelingen 2013-2014, 211), of de brief die de Privacycoalitie schreef aan de minister van Veiligheid en Justitie (Kamerstukken II 2013-2014, 32761, nr. 83). Daarnaast dragen ook publieksevents, workshops en websites bij aan het maatschappelijk debat over privacy en digitale rechten, en aan de vaardigheden die gebruikers nodig hebben om zichzelf te beschermen (bijvoorbeeld de online Toolbox Internetvrijheid van Bits of Freedom). Stichting Privacy First bewandelt een meer juridische weg om aandacht te vragen voor privacyschendingen, door procedures aan te spannen over onder andere de afname van vingerdrukken onder de Paspoortwet, trajectcontroles en de bewaarplicht voor telecomgegevens. Daarmee laat Privacy First zien dat ook maatschappelijke organisaties een rol kunnen spelen in handhaven van wetgeving en de bescherming van publieke belangen. Moerel en Prins (2016) stellen dat dit soort procedures belangrijk aanvulling kan zijn op handhaving door toezichthouders. In de privacy- en gegevensbescherming is er een toenemende aandacht voor zogenaamde *class actions* – procedures die namens een groep mensen worden aangespannen.

Ook de Consumentenbond is actief op het thema privacy, bijvoorbeeld door in kaart te brengen hoe fitnessapps met gebruikersgegevens omgaan. Met de campagne Digidwang verzet de Consumentenbond zich daarnaast tegen de trend dat steeds meer organisaties consumenten dwingen tot digitalisering. In november 2015 lanceerde de ANWB, samen met haar Europese zusterorganisaties, de campagne 'My car, my data' om het publiek bewust te maken en regelgeving te bepleiten over de data die fabrikanten van slimme auto's verzamelen.

### Maatschappij en bedrijfsleven

Maatschappelijke organisaties, zoals Platform voor de Informatiesamenleving ECP, vormen een link tussen de beleidswereld en het bedrijfsleven. ECP werkt samen met bedrijven en overheden om de maatschappelijke en economische waarde van informatietechnologie te versterken. Met campagnes, onderzoek en debat brengen ze stakeholders bijeen, en ondersteunen ze de uitvoering van bepaalde beleidsdoelstellingen. Een belangrijk thema is het stimuleren en verbeteren van digitale vaardigheden en digitale veiligheid, zowel bij bedrijven, overheden als consumenten. Dat gebeurde bijvoorbeeld met het programma Digiveilig Digivaardig, en de organisatie van het CodePact, een programma dat zoveel mogelijk kinderen de kans wil bieden om te leren programmeren.

Ook vanuit het bedrijfsleven worden acties ondernomen verantwoord om te gaan met de ethische kanten van de digitaliserende samenleving. Sommige bedrijven profileren zich expliciet met het aanbieden van privacyvriendelijke diensten. Zo werkt de QIY Foundation aan een systeem dat gebruikers meer controle over hun eigen data geeft. De zoekmachine Ixquick biedt mensen een mogelijkheid om te zoeken op het web zonder daarbij persoonlijke gegevens af te staan. Internetproviders zoals XS4All en Greenhost zetten zich in voor een open en vrij internet en digitale veiligheid. Daarnaast zijn er ook sector-brede initiatieven om maatschappelijke verantwoordelijkheid te nemen op het gebied van digitalisering. Een voorbeeld is het Verbond van Verzekeraars dat namens haar leden een convenant afsloot over de omgang met gegevens en jaarlijks de impact van big data op maatschappelijke solidariteit monitort (Verbond van Verzekeraars 2016). Tegelijkertijd is er ook regelmatig kritiek op bedrijven, bijvoorbeeld over de manier waarop ze met gegevens van gebruikers omgaan. Grote technologiebedrijven zoals Google, Apple of Facebook zijn daarin soms het mikpunt van kritiek of zorgen. Maar ook banken, verzekeraars, elektronica producenten of ontwikkelaars kwamen in de afgelopen jaren negatief in de publiciteit.<sup>84</sup> Hoewel hierboven besproken acties van bedrijven laten zien dat er in het bedrijfsleven een groeiende aandacht voor maatschappelijke en ethische vraagstukken rond digitale producten en diensten is, ontbreekt het nog aan structurele aandacht en verantwoordelijkheid voor de ethische en maatschappelijke impact van digitalisering.

### Internationaal

De onthullingen van klokkenluider Snowden over dataverzameling en surveillance door NSA en andere internationale veiligheidsdiensten hebben sinds 2013 voor veel maatschappelijke en politieke discussie gezorgd, en hebben de thematiek van surveillance en privacy nadrukkelijk op de maatschappelijke agenda gezet. Op internationaal niveau richten zich diverse campagnes en initiatieven van maatschappelijke organisaties zich op het beschermen en verankeren van digitale rechten. Om de rechten van internetgebruikers te beschermen, riep Berners Lee, de grondlegger van het wereldwijde web, op tot een digitale Magna Carta<sup>85</sup> (Kiss 2014). In het verlengde van deze oproep van Berners Lee zijn er in het Verenigd Koninkrijk initiatieven genomen om te komen tot een *Digital Bill of Rights*.<sup>86</sup> In aanloop naar de Europese Verkiezingen in 2014 lanceerde het European Digital Rights Initiative (EDRI) een verzameling burgerrechtenorganisaties, waaronder Bits of Freedom – een campagne over digitale rechten. En de door diverse internationale denktanks geïnitieerde Global Commission on Internet Governance roept op tot bescherming van fundamentele rechten van digitale burgers (GCIG 2016).

---

<sup>84</sup> Zie bijvoorbeeld <http://www.volkskrant.nl/tech/facebook-werkt-aan-censuurwapen-om-toegang-tot-china-te-krijgen-a4420772/>  
<http://www.volkskrant.nl/media/google-en-facebook-nemen-maatregelen-tegen-nepnieuws-na-kritiek-a4415610/>  
<http://www.volkskrant.nl/tech/achmea-biedt-korting-in-ruil-voor-privedata-a4154347/>  
<http://www.volkskrant.nl/tech/apple-music-bindt-in-na-protest-taylor-swift-a4085852/>  
<http://www.volkskrant.nl/tech/airbnb-uber-ze-hebben-maling-aan-alles-a3795584/>

Of in kamervragen, zie bijvoorbeeld Kamerstukken II, 2013-2014, aanhangselnummer 2008; Kamerstukken II, 2013-2014, aanhangselnummer 2912; Kamerstukken II, 2015-2016, aanhangselnummer 2377.

<sup>85</sup> De Magna Carta is een van de eerste verdragen waarmee in de middeleeuwen in Engeland de macht van de koning werd ingeperkt en een aantal fundamentele rechten werd vastgelegd. De Magna Carta wordt gezien als een belangrijke historische stap in de ontwikkeling van het moderne democratische stelsel.

<sup>86</sup> [cybersalon.org/digital-bill-of-rights-uk](http://cybersalon.org/digital-bill-of-rights-uk)

Behalve de maatschappelijke discussie over privacy tekent zich een discussie af omtrent autonome technologie. Daarin staan zaken als controle, transparantie en menselijke autonomie centraal, en wordt opgeroepen tot nieuwe vormen van toezicht. In februari 2016 pleitte innovatiestichting Nesta voor het instellen van een *Machine Intelligence Commission* in het Verenigd Koninkrijk (Mulgan 2016). Nesta baseert de aanbevelingen op de ervaringen met eerdere commissies voor milieuvervuiling en embryo-gebruik, die een belangrijke rol hebben gespeeld in het stimuleren van een maatschappelijk debat over ethische grenzen, het creëren en borgen van publiek vertrouwen, en het mogelijk maken van economische ontwikkeling. Zo'n commissie zou geen formele rol moeten hebben in het certificeren of goedkeuren van algoritmen, maar zou sterke bevoegdheden moeten hebben voor toegang tot informatie en het verrichten van onderzoek. Het Institute of Electrical and Electronics Engineers (IEEE) – de internationale organisatie voor technische professionals – werkt aan een initiatief om ontwikkelaars van autonome systemen te ondersteunen in het maken van ethisch verantwoorde keuzes (IEEE 2016). In september 2016 publiceerde het Britse Standards Institute (BSI) een set van richtlijnen voor ethisch verantwoord ontwerp en toepassing van robotica (BSI 2016) En ook bij sommige bedrijven worden commissies ingesteld om met ethische vragen om te gaan. Zo heeft de Rabobank een Bureau Ethiek waarin het onderwerp digitalisering aan de orde komt en stelde Google een ethische commissie voor de ontwikkeling van kunstmatige intelligentie. Over de rol en de samenstelling van de commissie van Google wordt echter niets naar buiten gebracht (Shead 2016).

### **Conclusie**

In Nederland spelen maatschappelijke organisaties – zoals Bits of Freedom, Privacy First, de Consumentenbond en ECP – en enkele maatschappelijk verantwoorde bedrijven een rol in de discussie over de effecten van digitalisering. Maatschappelijke kwesties die veel aandacht krijgen zijn privacy en digitale veiligheid en daarmee samenhangend digitale vaardigheden (zie ook tabel 5.2). Issues als digitale dwang en uitsluiting en het belang van een open en vrij internet krijgen ook aandacht. Vanuit het veld van maatschappelijke organisaties krijgen kwesties als rechtvaardigheid, autonomie en menselijke waardigheid nog relatief weinig aandacht.

Wat betreft technologie is er voornamelijk oog voor het internet, apps, overheidsdiensten en consumentenelektronica. Nederlandse maatschappelijke organisaties spelen nog geen duidelijke rol in het stimuleren van discussies over AI, robotica en opkomende technologieën. Dat komt mogelijk omdat zulke technologieën een nog weinig zichtbaar zijn in het alledaagse leven van mensen. Met de opkomst van robotica, slimme algoritmen en IoT kan dat op korte tot middellange termijn veranderen. Organisaties als ECP en bedrijven als Google zien in dat dergelijke nieuwe ontwikkelingen vragen om ethische reflectie over thema's zoals autonomie, datadiscriminatie en menselijke waardigheid. We zien internationaal de oprichting van ethische werkgroepen en commissies en een beginnende zoektocht naar ethische richtlijnen voor ontwikkelaars en bedrijven, zoals de initiatieven van de Institute of Electrical and Electronics Engineers (IEEE) en het Britse Standards Institute (BSI) laten zien. Ook wordt opgeroepen tot nieuwe vormen van toezicht. Met name de ontwikkeling dat technologie steeds autonomer wordt, roept de vraag op hoe de werking van slimme algoritmes valt te (blijven) controleren. Daarnaast tekent zich vanuit het maatschappelijke domein internationaal een discussie af over mensenrechten in het digitale

tijdperk, zoals initiatieven voor een *Digital Bill of Rights* in het Verenigd Koninkrijk laten zien. Daarbij staat het online domein centraal, en dan met name autonomie op het internet.

**Tabel 5.2** Activiteiten op maatschappelijk niveau

Wie / wat	Technologie	Issue	Actie
ECP	Digitalisering	Veiligheid, privacy	Programma's voor digitale skills en veiligheid, werkgroep ethiek & ICT
Bits of Freedom	Internet, digitale communicatie	Privacy, veiligheid	Big brother awards, privacycoalitie, internetvrijheid toolbox
Privacy First	Digitale communicatie, digitale overheid	Privacy	Juridische acties
Consumentenbond	Apps, consumententechnologie	Privacy, inclusiviteit	Campagne privacybewustzijn. Aanspreken producenten op privacy
<i>EU en internationaal</i>			
EDRi (EU)	Internet, digitale communicatie	Mensenrechten online	Campagne om belofte voor bescherming digitale rechten van parlements kandidaten
Nesta (VK)	AI, algoritmen, robotica	Autonomie, controle over technologie, vertrouwen	Oproep tot een Machine Intelligence Commission
Global Commission on Internet Governance (int.)	Internet, digitale communicatie	Mensenrechten online	Rapport met oproep tot bescherming digitale rechten
IETF (int.)	Internet, digitale communicatie	Mensenrechten	Human Rights Research Group die onderzoekt hoe in protocollen rekening gehouden kan worden met rechten
IEEE (int.)	AI, algoritmen, robotica	-	Initiatief om ontwerpers van autonome systemen te helpen ethische keuzes te maken

## 5.5 Agendavorming

We hebben hiervoor beschreven hoe in de domeinen van wetenschap, rechten en de maatschappij discussies over verschillende ethische en maatschappelijke aspecten naar voren komen. In het politiek-bestuurlijke domein worden deze signalen vanuit de wetenschap en maatschappij op de agenda gezet door adviesraden en instituten. Het onderwerp digitalisering komt bij veel organisaties aan bod, maar slechts een beperkt aantal kijkt ook naar gerelateerde ethische en maatschappelijke issues. Met name de Wetenschappelijke Raad voor het Regeringsbeleid (WRR), de Adviesraad Internationale Vraagstukken (AIV), Raad voor de leefomgeving en infrastructuur (Rli) en het Rathenau Instituut hebben de laatste jaren aandacht voor de relatie digitalisering, maatschappij en ethiek gevraagd. De vraag is daarbij of de ethische en maatschappelijke vraagstukken die worden gesignaleerd – zoals beschreven in hoofdstuk 3 – ook worden opgepikt in de agendavorming.

### Rol in het governancelandschap

De adviesraden en instituten leveren informatie en advies op verzoek van beleidsmakers of het parlement en brengen daarnaast ongevraagd adviezen uit om thema's op de agenda te zetten. De Rli en de AIV spreken zich specifiek uit over digitalisering in relatie tot hun werkdomein; respectievelijk de leefomgeving en buitenlands beleid op het gebied van mensenrechten, vrede en veiligheid. De WRR heeft als taak de regering te adviseren over langetermijnontwikkelingen die de samenleving beïnvloeden.<sup>87</sup> Vanuit die rol heeft de WRR in een aantal studies naar digitalisering gekeken. Het meest structureel komt het onderwerp aan bod in het werk van het Rathenau Instituut, dat als taak heeft bij te dragen aan het maatschappelijke en politieke debat over vraagstukken die samenhangen met wetenschappelijke en technologische ontwikkelingen, zoals digitalisering.<sup>88</sup> Met meer dan twintig studies is digitalisering voor het Rathenau Instituut in de laatste jaren een belangrijk thema geweest dat op verschillende wijzen is geagendeerd. Daarbij richt het instituut zich naast het politieke-bestuurlijke ook op het publieke debat over de impact van digitalisering.

### Gesignaleerde ethische en maatschappelijke vraagstukken

Zoals tabel 5.3 laat zien vragen de verschillende organisaties aandacht voor een groot aantal verschillende vraagstukken van digitalisering. De analyse in Appendix A laat zien dat alle ethische en maatschappelijke kwesties die we signaleerden in hoofdstuk 3 in algemene zin aan bod komen in de agendavorming. Ethische vraagstukken zoals privacy en veiligheid komen vaak terug, maar ook thema's zoals autonomie, menselijke waardigheid, sociale inclusie, transparantie, controle over technologie, rechtvaardigheid en discriminatie worden geagendeerd. Veelal worden deze kwesties aangekaart aan de hand van een bepaalde technologische ontwikkeling of praktijk, zoals big data, robotisering, de digitale overheid of autonome wapentechnologie.

### Governance-opties

In de verschillende rapporten en adviezen zien we grofweg drie typen aanbevelingen over de governance van de ethiek van digitalisering: versterken van de beleidsvorming en -bepaling en politieke discussie; versterken van het toezicht; en versterken van de maatschappelijke discussie

---

<sup>87</sup> Instellingswet WRR, art. 2.a 30 juni 1976

<sup>88</sup> Staatscourant. 2009, 11024



over technologie.<sup>89</sup> Diverse studies vragen om kabinetsbrede visievorming op terreinen als big data, internet, robotica en intieme technologie. Ze benadrukken de behoefte aan een interdepartementale aanpak. De AIV doet dat in relatie tot internetbeleid (AIV 2014), de Rli in relatie tot data en digitalisering (Rli 2014). Het Rathenau Instituut roept op tot visievorming op het gebied van robotica (Van Est & Royakkers 2012) en intieme technologie (Van Est & Rerimassie 2014). Daarnaast adviseren diverse raden om op het gebied van big data en algoritmen toezicht te versterken (WRR 2016; AIV 2014; Dratwa 2014). De WRR (2016) signaleert dat er een mismatch is tussen big data en de huidige wetgeving die zich voornamelijk richt op het verzamelen van gegevens. Net als het Rathenau Instituut (Van 't Hof et al. 2012b; Kool et al. 2015) stelt de WRR dat er meer aandacht nodig voor de fase van data-analyse en hoe toepassingen van deze data-analyses het individu raken.<sup>90</sup> Dit sluit aan bij wat er in het wetenschappelijk domein wordt gesignaleerd en toont daarmee ook de link tussen het domein van wetenschappelijke kennis en het domein van de agendavorming. Tot slot pleiten verschillende instanties in hun rapporten voor het stimuleren van maatschappelijk debat en het versterken van mediawijsheid en technologisch burgerschap (bijvoorbeeld Rli 2015; Van Est & Rerimassie 2014).

Op Europees niveau houdt de European Group on Ethics in Science and New Technologies (EGE) zich sinds haar oprichting in 1991 bezig met ethische vraagstukken omtrent nieuwe technologie. Aanvankelijk gebeurde dat vooral op het gebied van biotechnologie en medisch onderzoek, maar de laatste jaren is de EGE zich meer met ethische kwesties op het vlak van informatietechnologie gaan bezighouden. Met rapporten over de ethische aspecten van ICT (Salvi 2012) en surveillance (Dratwa 2014) pleit de EGE voor bescherming van fundamentele rechten in het digitale tijdperk.

### **Conclusie**

De ethische en maatschappelijke kwesties die we signaleerden in hoofdstuk 3 worden in het politiek-bestuurlijke domein voor het overgrote deel ook geagendeerd door het bestaande stelsel van adviesraden en instituten, zoals ook zichtbaar wordt in tabel 5.3. De verschillende adviesraden en instituten vervullen daarin vanuit hun instellingsbesluit een eigen rol. Behalve vraagstukken omtrent privacy en dataverzameling worden ook belangrijke vragen omtrent rechtvaardigheid, autonomie, controle over technologie en menselijke waardigheid op de agenda gezet. De meeste adviezen met betrekking tot beleid richten zich – vanuit de opdracht van de adviesraden en instituten – op specifieke technologische praktijken zoals zorgtechnologie of cyberintelligentie. Dat roept de vraag op hoe de overheid een integrale visie vormt op digitalisering, een vraag die ook terugkomt in adviezen tot visievorming en interdepartementale afstemming.

---

<sup>89</sup> Zie voor een beschrijving van de verschillende adviezen de uitgebreide analyse in Appendix A.

<sup>90</sup> Bijvoorbeeld hoe het individu anders wordt behandeld op basis van groepsprofielen en hoe hij wordt beschermd tegen onjuiste analyses.

**Tabel 5.3** Activiteiten binnen het politiek-bestuurlijk domein op het gebied van agendavorming

Wie/wat	Technologie	Issue	Advies/actie
<i>Wetenschappelijke Raad voor het Regeringsbeleid</i>			
iOverheid	Digitaliserende overheid	privacy, transparantie, autonomie, controle	Besef van transformerende impact van ICT op overheid. Instellen iAutoriteit en iPlatform voor weerbaarheid van burgers
Publieke kern van het Internet	Internet infrastructuur	veiligheid, censuur, vrije toegang	Publieke kern van het internet vastleggen in internationale verdragen
Robot de Baas	Robotica	werk, inclusie, gelijkheid, autonomie	Inzetten op complementaire samenwerking mensen en robotica
Big data in een vrije & veilige samenleving	Big data en algoritmen	privacy, veiligheid, autonomie, discriminatie, recht op eerlijk proces	Sterkere focus op het gebruik van gegevens, toezicht op algoritmen, nieuwe taken voor toezichhouders
<i>Adviesraad internationale vraagstukken</i>			
Het internet	Internet- infrastructuur	Internetvrijheid, privacy, surveillance, informatieveiligheid	Beschermen internetvrijheid. Interdepartementale coördinatie en visie op internetbeleid
Autonome wapensystemen	Autonome wapensystemen	controle over technologie, verantwoordelijkheid	Betekenisvolle menselijke controle bij inzet autonome wapensystemen
<i>Raad voor de leefomgeving en infrastructuur</i>			
Technologische innovaties in de leefomgeving	Digitalisering (AI, data-infrastructuur, drones, robotica, IoT, VR)	privacy, transparantie, veiligheid, toegang, controle op algoritmen, autonomie	Data-ontwikkeling vraagt kabinetsbrede visie en maatschappelijke debatten over impact op fundamentele waarden
<i>Rathenau Instituut (selectie van publicaties)</i>			
Just Ordinary Robots	Robotica, AI	privacy, autonomie, menselijke waardigheid, controle over technologie	Beleidsvisie op welke taken er kunnen worden overgedragen aan robots, beslissen over leven of dood niet automatiseren
Werken aan de Robotsamenleving	Robotica, AI, platformen	werkeloosheid, menselijke waardigheid, inclusiviteit	Scholing, inclusieve innovatie, waarborgen tegen monopolisering en uitbuiting digitale platformen
De datagedreven samenleving	Big data, algoritmen	privacy, transparantie, controle op algoritmen, autonomie, discriminatie, machtsverhoudingen	Controle op algoritmen, bescherming van autonomie en gelijkheid. Data zijn niet neutraal: stimuleren van data-geletterdheid
Eerlijk advies	Health apps, wearables, persuasieve technologie	privacy, autonomie, betrouwbaarheid van technologie, transparantie, machtsverhoudingen	Beschermen privacy en autonomie, keurmerk voor betrouwbare e-coaches, verplichte bewijslast voor overheidsinzet gedragsbeïnvloeding
Intieme technologie	Digitalisering breed	privacy, autonomie, menselijke waardigheid	Rijksbrede aanpak op de impact van digitalisering op grondrechten,

			bevorder technologisch burgerschap
<i>European Group on Ethics in Science and New Technologies</i>			
Ethics of Information and Communication Technologies	Digitalisering breed	privacy, menselijke waardigheid, autonomie, vrijheid van meningsuiting, toegang tot technologie	Toegang tot ICT. Stimuleren digitale vaardigheden, vrije online identiteitsontwikkeling en verantwoord persoonlijk gebruik van ICT
Ethics of Security and Surveillance Technologies	Big data, surveillance-veiligheids-technologie	veiligheid, privacy, menselijke waardigheid, autonomie, discriminatie	Verplicht expliciet maken assumpties van algoritmen. Menselijke waardigheid niet uitruilen voor andere waarden zoals veiligheid

Rathenau Instituut

## 5.6 Beleidsvorming en -bepaling

In de fase van beleidsvorming en -bepaling vindt de vertaling van de beleidsvoorbereidende rapporten en adviezen naar visies, beleid, regelgeving en wetten plaats, en de politieke accordering daarvan. We kijken hier naar de actoren die institutioneel verantwoordelijk zijn voor het beleid en politieke besluitvorming: het kabinet, de ministeries en het parlement bestaande uit de Eerste en de Tweede Kamer.

Op het niveau van beleidsvorming en -bepaling zien we in tabel 5.4 dat vraagstukken omtrent privacy, databescherming en veiligheid een prominente plaats innemen. In de Eerste en Tweede Kamer worden er regelmatig vragen gesteld over de bescherming van privacy en visievorming over het onderwerp (zie Appendix A). Vanuit de departementen worden er verschillende acties ondernomen. Bijvoorbeeld het versterken van de capaciteiten van de Autoriteit Persoonsgegevens. Naast het vergoten van de boetebevoegdheid komt herhaaldelijk de roep naar voren om ook het budget van de Autoriteit Persoonsgegevens te vergroten.<sup>91</sup> Nieuwe wet- en regelgeving – op nationaal en op Europees niveau – versterkt de bescherming van het individu, maar de capaciteit en bevoegdheid van de toezichthouder blijft een belangrijk onderwerp van discussie: is deze wel voldoende toegerust om met uitdagingen van big data, profilering en slimme algoritmen om te gaan? Continue scholing en opleiding wordt vaak als oplossing genoemd om de uitdaging van digitalisering het hoofd te bieden. Zo stelt het Ministerie van Onderwijs, Cultuur en Wetenschappen in haar brief omtrent Onderwijs 2032 dat digitale vaardigheden onderdeel van het kerncurriculum van het onderwijs moeten worden (Kamerstukken II, 2015-2016, 31293, nr. 278). In de brief over toekomstbestendige regelgeving komt de spanning naar voren tussen het scheppen van ruimte voor innovatie terwijl er ook oog wordt gehouden voor de bescherming van publieke waarden (Kamerstukken II 2014-2015, 33009, nr.10).

De ministeries en het parlement vragen actief om advies over hoe ze met nieuwe technologische ontwikkelingen om moeten gaan. Denk aan de aanvraag van de ministerraad om een advies over

<sup>91</sup> Zie bijvoorbeeld Kamerstukken II 2015-2016 32 761, nr. 102

big data en veiligheid bij de WRR, de adviesaanvraag van het Ministerie van Sociale Zaken en Werkgelegenheid richting de SER over robotisering en arbeid en het instellen door het Ministerie van Economische Zaken van de high level expert group voor big data en profiling, die moest kijken naar de impact van deze ontwikkelingen op het grondrecht op privacy en het grondrecht op gelijke behandeling. Ook binnen het parlement leeft de wens om goed geïnformeerd over de maatschappelijke en ethische aspecten van digitalisering te debatteren. Op het gebied van technologie en arbeid verzocht de Tweede Kamer het Rathenau Instituut studie de wetenschappelijke kennis op een rij te zetten. De motie Ester c.s. (Kamerstukken I, 2013-2014, 33750 XIII) verzoekt het Ministerie van Economische Zaken om jaarlijks te rapporteren over de rol van ethiek in het innovatiebeleid en probeert daarmee een structureel terugkerende politiek-ethisch debat in de Eerste Kamer mogelijk te maken. De motie Ester laat net als de motie Gerkens zien dat het Eerste Kamer de impact van digitalisering en het belang van reflectie daarop onderkent.

Het parlement vraagt de regering regelmatig een overkoepelende visie op de impact van digitalisering te vormen, bijvoorbeeld over privacy (bijvoorbeeld Kamerstukken II 2013-2014, 32761, nr. 83; Kamerstukken II 2013-2014, 32761, nr. 89). D66 stelt in haar Techvisie dat het huidige beleid te veel incident-gedreven is en beveelt aan een minister van Economie, Technologie en Privacy in te stellen. Het idee van een overkoepelende aanpak van het onderwerp digitalisering komt ook terug in de internationale initiatieven om digitale rechten vast te leggen. Bijvoorbeeld in het *Republique-Numerique*-wetsvoorstel in Frankrijk en de oproep voor een *Digital Bill of Rights* in het Verenigd Koninkrijk. In het buitenland zien we ook aandacht voor ethische aspecten die verband houden met de opkomst van de zelfsturende auto. De Duitse minister van Transport heeft op dat terrein een ethische commissie ingesteld (Ramthun & Schlesiger 2016) en in de Verenigde Staten heeft de federale regering regels opgesteld voor (sterk) geautomatiseerde voertuigen, waarin aandacht gevraagd wordt voor ethische vraagstukken (USDOT 2016). Om de Europese Commissie aan te zetten tot actie op het gebied van maatschappelijke en ethische aspecten van robotisering en AI werkt de Commissie Juridische Zaken van het Europees Parlement aan een rapport over robotica en kunstmatige intelligentie (2015/2103(INL)). Het conceptrapport bevat een voorstel voor een ethische code voor robotbouwers, een code voor commissies betreffende onderzoeksethiek en een model voor gebruikers over toegestane handelingen met robots.

## **Conclusie**

We zien dat in de fase van beleidsvorming en -bepaling relatief veel aandacht voor privacy is. Ministeries en het parlement zoeken actief naar informatie over nieuwe technologische ontwikkelingen en hoe hier vanuit beleidsoogpunt mee om moet worden gegaan: welke nieuwe verantwoordelijkheden de digitalisering met zich meebrengt en hoe innovatie de ruimte kan krijgen met oog voor publieke waarden. Het parlement wil door de regering op dit gebied goed geïnformeerd worden, zodat een goed parlementaire debat mogelijk wordt. Vanuit de Eerste en Tweede Kamer zien we ook regelmatig de vraag aan de regering om een integrale visie te vormen op gebieden zoals privacy.

De politiek-bestuurlijke aandacht voor vraagstukken omtrent autonomie, rechtvaardigheid en menselijke waardigheid is nog relatief gering, maar lijkt groeiende. Met name door big data, de inzet algoritmen, autonome wapensystemen en zelfsturende auto's worden vraagstukken zoals rechtvaardigheid, discriminatie en autonomie in de publieke discussie meer zichtbaar. In het buitenland zien we dat op diverse terreinen langzaam politiek-bestuurlijke stappen gezet worden,

bijvoorbeeld door hiervoor genoemde Commissie Juridische Zaken van het Europees Parlement (zie ook tabel 5.4).

**Tabel 5.4** Activiteiten binnen het politiek-bestuurlijk domein op het gebied van beleidsvorming.

Wie/wat	Technologie	Issue	Actie
<i>Ministerie van Economische Zaken</i>			
Visie Telecommunicatie	Internet, digitale communicatie	Vrij, open internet, keuzevrijheid	Stimuleren van veiligheid, neutraliteit en continuïteit
Brief big data en profilering	Big data, profilering, algoritmen	Privacy en gelijke behandeling	High level expert group
Brief toekomstbestendige regelgeving	Digitale platformen	Publieke waarden zoals consumetenveiligheid, eerlijke concurrentie	Experimenteeruimte in regelgeving met oog voor publieke waarden.
Brief ethische aspecten van het innovatiebeleid	Digitalisering	Versmelting mens & tech; privacy en autonomie	Aandacht voor ethiek in onderzoek; jaarlijkse rapportage bedrijvenbeleid
<i>Ministerie van Veiligheid en Justitie</i>			
Commissie Brouwer-Korf	Digitalisering, digitale communicatie	Veiligheid en privacy	Meldplicht datalekken; uitbreiding boetebevoegdheid AP
Notitie vrijheid & veiligheid in de digitale samenleving	Digitalisering, digitale communicatie	Veiligheid en privacy	Stimuleren privacy by design, verplichte <i>Privacy Impact Assessment</i> voor nieuwe wetgeving, campagne voor digitale weerbaarheid. Aanvraag WRR advies big data
Wetsvoorstel computercriminaliteit III	Digitalisering	Veiligheid	Nieuwe bevoegdheden veiligheidsdiensten
Kabinetsstandpunt encryptie	Encryptie	Vertrouwelijke communicatie, privacy	Wettelijke beperking op encryptie niet wenselijk
<i>Ministerie van Onderwijs, Cultuur en Wetenschap</i>			
Brief Onderwijs 2032	Digitalisering, robotisering	Digitale vaardigheden, privacy, veiligheid, online omgangsvormen	Digitale geletterdheid in het kerncurriculum van het onderwijs. Continue scholing
<i>Ministerie van Sociale Zaken en Werkgelegenheid</i>			
Brief Technologische ontwikkelingen en arbeidsmarkt	Robotisering, automatisering	Menselijke waardigheid, technologische werkeloosheid	Aanvraag onderzoek Rathenau, SER, CPB
Brief Werken aan de robotsamenleving	Robotisering, automatisering	Menselijke waardigheid, technologische werkeloosheid	Inzetten op goede opleidingen, leven lang leren, omscholing en transities
<i>Ministerie van Buitenlandse Zaken</i>			

Brief Buitenlands internetbeleid	Internet	Fundamentele rechten: vrijheid, privacy, gelijkheid	Interdepartementale visie op internetbeleid, fundamentele rechten gelden ook online
Mensenrechten-rapportage 2015	Internet, algoritmen	Fundamentele rechten: vrijheid, privacy, gelijkheid	Aandacht voor digitale rechten, ethiek en algoritmen op GCCS Conferentie
Brief Autonome wapensystemen	Autonome wapensystemen	Menselijke waardigheid, controle over technologie	Toewijzing verantwoordelijkheid onderdeel van ontwerpfase. AIRCW toetsing op betekenisvolle controle

*Ministerie van Binnenlandse Zaken*

Brief iOverheid	Digitalisering van de overheid	Weerbaarheid burgers, controle over technologie	Besef impact digitalisering verankeren bij de overheid
Wetsvoorstel Wiv	Digitalisering communicatie	Veiligheid	Nieuwe bevoegdheden veiligheidsdiensten

*Parlement*

Kamervragen en moties	Verschillende deelaspecten digitalisering	Verschillende ethische kwesties, veel aandacht voor privacy	Vragen om visie, standpunten, beleid, wet en regelgeving
VVD Robotagenda	Robotisering	Menselijke waardigheid; werkeloosheid	Inzetten op educatie. Onderzoek waarde van een Nationale Ethiek Commissie
D66 Techvisie	Digitalisering, internet	Privacy, surveillance, netneutraliteit, veiligheid, vertrouwelijke communicatie	Minister van Economie, Technologie en Privacy, digitale vaardigheden, versterking toezichhouders, zorgplicht internetreuzen

*EU en internationaal*

EU – Onlife initiative	Digitalisering breed	Breed aantal ethische vraagstukken	Onlife Manifesto informeert onderzoeksagenda
EU – Algemene Verordening Gegevensbescherming	Dataverzameling en bescherming	Privacy, databescherming, transparantie	Versterking toezichthouder. Versterking rechten internetgebruiker en plichten dataverwerker
European Parliament – Draft Report on Civil Law rules on Robotics	Robotisering en kunstmatige intelligentie	Veiligheid, privacy, integriteit, menselijke waardigheid en autonomie	Voorstel voor een resolutie voor het Europees Parlement om ethische principes en een Europees Agentschap voor robotica en AI te creëren
Verenigd Koninkrijk – Campagne voor Digital Bill of Rights	Digitalisering, internet, digitale communicatie	Privacy, surveillance, machtsverhoudingen	Voorstel voor recht op eigenaarschap gegevens. Gelijke toegang internet

Frankrijk – Wetsvoorstel Republique Numerique	Digitalisering, internet, platformen digitale communicatie	Privacy, netneutraliteit, transparantie, machtsverhoudingen	Recht om vergeten te worden. Transparantie over verdienmodellen platformen. Rechten op data na overlijden
---	--	---	---

---

Rathenau Instituut

## 5.7 Beleidsuitvoering

In de fase van beleidsuitvoering kijken we naar de manier waarop toezichthouders en toetsingscommissies ervoor zorgen dat de regels, normen en wetten worden geïmplementeerd en nageleefd die in de fase van beleidsvorming en -bepaling zijn vastgelegd. Een toezichthouder is een door de overheid aangesteld, onafhankelijk en onpartijdig instituut dat toeziet op naleving van wet- en regelgeving. Toetsingscommissies voeren op basis van regelgevende kaders en protocollen, meestal casus voor casus, een toets uit of een bepaalde actie – zoals de aanschaf van een autonoom wapensysteem – conform de gestelde kaders is.

### Van dataprotectie naar digitale ethiek

Een toezichthouder die een duidelijke rol speelt bij digitalisering is de Autoriteit Persoonsgegevens. Het toezicht van de AP is specifiek gericht op privacy en gegevensbescherming. Vanuit die rol speelt de toezichthouder een belangrijke rol in het evalueren van nieuwe wetgeving, en het controleren van privacybeleid. Per 1 januari 2016 zijn het budget en de bevoegdheden van de AP uitgebreid, onder andere met een sterkere boetebevoegdheid en het toezicht op de meldplicht datalekken (AP 2016). De AP stelt goed geïnformeerde toestemming en controle door de gebruiker centraal. We zien in onze analyse dat big data en de opkomst van het Internet of Things dit perspectief onder druk zetten. Ook zien we voorstellen dat de AP een sterkere rol moet spelen in het toezicht op toepassingen van big data en algoritmen: de WRR (2016) adviseert de capaciteiten van de AP en de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) op dit vlak te versterken.

De Europese toezichthouder gegevensbescherming (EDPS), heeft haar blikveld verbreed tot buiten het domein van de privacy. Met de opinie *Towards a new digital ethics* (EDPS 2015) en het instellen van een *Ethics Advisory Group* onderzoekt ze de verhouding tussen mensenrechten en digitale technologieën, zoals algoritmen, AI, big data en het Internet of Things. Met deze stap naar digitale ethiek komen issues zoals discriminatie, menselijke waardigheid en autonomie duidelijker op het netvlies van de Europese toezichthouder. In Nederland heeft het College voor de Rechten van de Mens (CRvDM) een rol waar het gaat om discriminatie en de bescherming van mensenrechten. In het strategisch plan van het CRvDM wordt echter nog niet gerefereerd aan de manier waarop technologische ontwikkelingen aan mensenrechten raken (CRvDM 2016).

Op het vlak van digitale veiligheid vervullen het Nationaal Cyber Security Centrum en de Cybersecurity Raad een duidelijke rol in het stimuleren van een veilige en weerbare digitale samenleving. Toezichthouders zoals de CTIVD en de Adviescommissie Internationaal Recht en

Conventioneel Wapengebruik vervullen een functie op een specifiek deelterrein, respectievelijk de veiligheidsdiensten en wapengebruik. De Autoriteit Consument en Markt (ACM) besteedt aandacht aan de bescherming van de digitale consument en geeft vanuit die hoedanigheid onder andere aandacht aan het onderwerp privacy. Daarnaast geeft de ACM aan te zullen kijken naar hoe bedrijven dankzij het gebruik van persoonsgegevens hun machtspositie op het internet vergroten. Daarmee kan ze een rol spelen in discussies omtrent monopolievorming bij platformen zoals Airbnb en Facebook en een *lock-in effect* dat ontstaat wanneer gebruikers niet gemakkelijk genoeg van de ene naar de andere aanbieder kunnen overstappen. Ook andere toezichthouders, waarvoor digitalisering traditioneel geen onderwerp is geweest, krijgen hiermee te maken. De Inspectie Leefomgeving en Transport werd bijvoorbeeld geconfronteerd met de opkomst van Uber en besloot dat de dienst UberPop, waarbij chauffeurs rijden zonder taxilicentie, niet is toegestaan in Nederland. Doordat verschillende toezichthouders met digitalisering te maken hebben, is het ook van belang dat er tussen de verschillende partijen afstemming plaatsvindt – zoals via het markttoezichthoudersberaad – over de manier waarop het toezicht wordt georganiseerd en waar verantwoordelijkheden voor de verschillende toezichthouders liggen.<sup>92</sup>

### Conclusie

Ons onderzoek laat zien dat voor de onderwerpen privacy en gegevensbescherming het toezicht het sterkst is ontwikkeld. Voor andere ethische kwesties omtrent digitalisering, zoals discriminatie, autonomie, menselijke waardigheid en ongelijke machtsverhoudingen bestaat er niet zo'n sterk georganiseerd toezicht. Het CRvdM is het aanspreekpunt voor discriminatie, maar digitalisering maakt geen nog expliciet deel uit van de agenda (CRvdM 2016). Tegelijkertijd lijkt er wel toenemende aandacht voor andere thema's dan privacy te ontstaan. Het meest sprekende voorbeeld hiervan zijn de initiatieven van de Europese toezichthouder gegevensbescherming (EDPS), met name de oprichting van een ethische adviesgroep.

Zowel in de maatschappelijke als in de politieke discussie komt de roep om sterker en breder toezicht naar voren, bijvoorbeeld als het gaat om toezicht op algoritmen. In paragraaf 5.4 bespreken we al dat de Britse innovatiestichting Nesta in 2016 opriep tot de oprichting van een Machine Intelligence Commission, die sterke bevoegdheden zou moeten krijgen om onderzoek te verrichten naar de werking van algoritmen en toegang tot informatie te krijgen.

**Tabel 5.5** Activiteiten binnen het politiek-bestuurlijk domein op het gebied van beleidsuitvoering.

Wie/wat	Technologie	Issue	Actie
AP	Digitalisering (diensten die persoonlijke gegevens verwerken)	Privacy, gegevensbescherming	Toezicht gegevensverwerking overheid en bedrijfsleven
ACM	Internet, apps	Privacy, machtsverhoudingen	Bewustwordingcampagne privacy, macht internetaanbieders

<sup>92</sup> Tijdens het markttoezichthoudersberaad werd bijvoorbeeld al eerder aandacht besteed aan het onderwerp Big data, zie <https://www.acm.nl/nl/publicaties/publicatie/13819/Agenda-Markttoezichthoudersberaad-2015/>



CRvdM	-	Mensenrechten (speciale aandacht discriminatie)	-
CTIVD	Veiligheidstechnologie	Privacy, gegevensbescherming, veiligheid	Toezicht op veiligheidsdiensten
NCSC / CSR	Digitalisering	Veiligheid	Stimuleren veilige en weerbare digitale samenleving
AIRCW	Wapentechnologie	Autonomie, controle over technologie, menselijke waardigheid	Advies over betekenisvolle menselijke controle bij wapensystemen
Nationale ombudsman	Digitale overheidsdiensten	Autonomie, menselijke waardigheid	Klachten bij systemen van de digitale overheid die in de fout gaan
<i>EU en internationaal</i>			
EDPS	Digitalisering (diensten die persoonlijke gegevens verwerken)	Verbreding van privacy naar autonomie, menselijke waardigheid, discriminatie	Adviesgroep digitale ethiek, verkenning impact van digitalisering op mensenrechten

Rathenau Instituut

## 5.8 Conclusie

In dit hoofdstuk hebben we onderzocht op welke plekken er in de governance van ethische en maatschappelijke aspecten van digitalisering blinde vlekken zitten. We hebben gekeken of de issues die we in hoofdstuk 3 hebben gesignaleerd afdoende worden geadresseerd in verschillende domeinen van het governance-ecosysteem. Daarbij keken we naar actoren op het gebied van: grond- en mensenrechten, wetenschap, maatschappij en politiek en bestuur. Deze concluderende paragraaf schetst een integraal beeld vanuit de vraag: welke vraagstukken worden gesignaleerd en geagendeerd; en zijn de betrokken actoren voldoende in staat om met deze issues om te gaan?

### **Inhoudelijke aandacht voor maatschappelijke en ethische vraagstukken rond digitalisering**

De opkomst van het Internet of Things, robotica, biometrie, persuasieve technologie, big data, digitale platformen, kunstmatige intelligentie, augmented en virtual reality, vormt een nieuwe digitaliseringsgolf. De informatiesamenleving komt daarmee in een nieuwe fase terecht; een fase die nieuwe maatschappelijke en ethische vraagstukken met zich meebrengt op het gebied van privacy, veiligheid, autonomie, rechtvaardigheid, menselijke waardigheid, controle over technologie en machtsverhoudingen. Onze analyse laat zien dat op dit moment de meeste publieke en politieke aandacht uitgaat naar de kwesties privacy (met name bescherming persoonsgegevens) en digitale veiligheid. Op dit vlak liggen er belangrijke uitdagingen zoals het zoeken naar een digitaal huisrecht en de bescherming van persoonlijke levenssfeer met de opkomst van het Internet of Things. We zien ook een groeiende aandacht voor de kwesties rechtvaardigheid en machtsverhoudingen. Met

betrekking tot de eerste kwestie is er aandacht voor big data en algoritmische profilering en de invloed op het recht op gelijke behandeling en de presumpctie van onschuld. Daarnaast is er groeiende discussie over de machtspositie van grote internetbedrijven. Voor de onderwerpen autonomie, menselijke waardigheid en controle over technologie is nog beperkte aandacht; in het maatschappelijke debat wordt het onderwerp nog beperkt opgepikt door maatschappelijke organisaties en ook in de fase van beleidsvorming en -bepaling is er nog weinig aandacht. Dat betekent dat er zich op dit vlak in het governancelandschap blinde vlekken bevinden. Deze vraagstukken worden gesignaleerd in de wetenschap en in de fase van agendavorming naar beleidsmakers gecommuniceerd, maar worden verder dus nog niet voldoende opgepikt. Hieronder gaan we per domein verder in op deze conclusies.

### **Wetenschap**

Binnen de wetenschap is er duidelijk aandacht voor de maatschappelijke en ethische kant van de golf van nieuwe digitale technologieën (zie hoofdstuk 3). Sommige wetenschappers proberen ook via de media publieke en politieke aandacht voor diverse kwesties omtrent digitalisering te vragen. Prominente wetenschappers zoals Hawking (Hawking et al. 2014) vragen bijvoorbeeld aandacht voor de impact van ontwikkelingen in de kunstmatige intelligentie. Vanuit haar kennispositie heeft de wetenschap een verantwoordelijkheid om deze risico's te agenderen. De Koninklijke Nederlandse Academie van Wetenschappen (KNAW) raadt aan om een *Ethical Review Board Informatics* in te stellen om te beoordelen of er bij informaticaonderzoek op een verantwoorde manier met persoonlijke gegevens om wordt gegaan. Sinds het begin van deze eeuw wint ook de notie van maatschappelijk verantwoord innoveren aan populariteit. Het doel daarvan is om al in de onderzoeksfase rekening te houden met maatschappelijke en ethische vraagstukken van nieuwe digitale toepassingen.

### **Grond- en mensenrechten**

De discussie over grondrechten in het digitale tijdperk kent inmiddels een lange geschiedenis. In het historisch hoofdstuk zagen we dat de discussie over privacy al sinds de volkstelling van 1971 speelt. In de jaren negentig kreeg dit debat met de opkomst van het internet en digitale diensten een nieuwe dimensie. Inmiddels worden we geconfronteerd met een nieuwe golf digitale technologieën, zoals het Internet of Things, robotica, big data en AI. Op internationaal niveau tonen initiatieven van de Raad van Europa, de VN en de UNESCO dat deze ontwikkelingen vanuit mensenrechtenperspectief aandacht behoeven. De analyse laat zien dat in Nederland de discussie over de borging van de grondrechten in relatie tot deze nieuwe golf digitale technologieën nog van de grond moet komen. Hier bevindt zich dus een blinde vlek in het governancelandschap. Het vraagt om beleidsmatige aandacht voor de borging van de grondrechten in relatie tot digitalisering waarin actief de verbinding gezocht kan worden met lopende Europese initiatieven die invulling geven aan de bescherming van fundamentele rechten in relatie tot digitalisering.

### **Maatschappij**

Diverse maatschappelijke organisaties houden zich bezig met privacy en digitale veiligheid en weten op dit terrein ook de politiek-bestuurlijke discussie aan te jagen. Acties van Bits of Freedom (zoals de Big Brother Award) en de Privacycoalitie leidden tot diverse Kamervragen. Nederland kent echter geen gevestigde maatschappelijke organisaties die discussies rond AI, robotica en opkomende technologieën, en rond ethische vraagstukken omtrent autonomie,

discriminatie en menselijke waardigheid aankaarten. Op internationaal niveau zien we meer beweging op dit terrein. Er zijn er verschillende internationale initiatieven om digitale rechten te beschermen en vast te leggen, zoals de actie voor een *Digital Bill of Rights* in het Verenigd Koninkrijk. Daarnaast zijn er ook tal van specifieke acties. De Britse innovatiestichting NESTA pleitte voor het oprichten van een commissie die toezicht houdt op algoritmen (Mulgan 2016). De Britse standaardisatieorganisatie ontwikkelde ethische richtlijnen voor ontwerpers van autonome systemen en robotica (BSI 2016). Bedrijven zoals Google richtten interne ethische commissies op om toe te zien op de ontwikkeling van AI. Hoewel deze initiatieven van bedrijven tonen dat de aandacht voor de impact van digitalisering groeit, ontbreekt het nog aan structurele aandacht en verantwoordelijkheid vanuit het bedrijfsleven om publieke waarden te borgen. Dat leidt tot een blinde vlek waar het gaat om de verantwoordelijkheden van bedrijven bij de governance van maatschappelijke en ethische kwesties van digitalisering. Daarnaast zorgt het ontbreken van een kritisch maatschappelijk tegengeluid over nieuwe digitaliseringsgolf – en de mogelijkheden van burgers en maatschappelijk middenveld om dit te organiseren – ook voor een blinde vlek in het maatschappelijk domein van het governancelandschap.

### **Politiek-bestuurlijk domein**

De ethische en maatschappelijke vraagstukken die de wetenschappelijke literatuur signaleert, worden tevens politiek-bestuurlijk geagendeerd. Hierbij spelen een breed palet aan technologische ontwikkelingen en praktijken een rol: van de opkomst van de slimme auto, big data en profilering tot en met bewapende militaire drones. Het Rathenau Instituut heeft hierin zelf een specifieke rol, en ook andere adviesorganen leveren vanuit hun institutionele rol een belangrijke bijdrage met adviezen en rapporten. Daarmee zien we dat de issues die in de wetenschap worden gesignaleerd ook in de fase van agendavorming terug te vinden zijn.

De stap van agendavorming naar beleidsvorming blijkt nog een uitdaging. Niet alle geagendeerde vraagstukken zien we ook terug in beleidsvorming. De meeste aandacht gaat hier op dit moment uit naar het vraagstuk van privacy. De nieuwe Algemene Verordening Gegevensbescherming biedt een duidelijk wettelijk kader op het gebied van gegevensbescherming. Voor de bescherming van privacy als mensenrecht is controle over persoonsgegevens alleen echter niet toereikend. Ook voor digitale veiligheid is aandacht, bijvoorbeeld in een nationale cybersecurity-strategie. Voor de overige gesignaleerde kwesties is er relatief weinig aandacht en daar waar er aandacht is, is er met name behoefte aan kennis over wat er technologisch speelt en wat daarvan de maatschappelijke en ethische betekenis kan zijn. De moties van Gerkens c.s. en Ester c.s. laten zien dat ook het parlement behoefte heeft aan een betere discussie over de maatschappelijke en ethische aspecten van digitalisering, en aan een structurele inbedding van deze discussie in de agenda van de Kamer.

Toezichthouders worden uitgedaagd te reageren op de trend van digitalisering. Digitalisering roept de vraag op of huidige toetsingsinstanties nog in staat zijn hun taak uit te voeren, en of hun mandaat nog adequaat is. De Autoriteit Markt & Consument gaat zich bijvoorbeeld bezig houden met de vraag hoe om te gaan met de sterke marktpositie van grote internetbedrijven. Als aanspreekpunt voor discriminatie heeft het College van de Rechten van de Mens echter (nog) weinig aandacht voor bijvoorbeeld datadiscriminatie. In het politieke debat zien we de roep om meer armslag voor de Autoriteit Persoonsgegevens (AP) en nieuwe vormen van toezicht, zoals toezicht op algoritmen. Illustratief is ook het initiatief van de Europese toezichthouder

gegevensbescherming (EDPS) om een *Ethics Advisory Group* in te stellen. Daarmee stelt de toezichthouder zelf de vraag hoe zij met ethische vragen zoals autonomie, discriminatie en menselijke waardigheid om moet gaan.

Aldus zien we in het politiek bestuurlijke domein verschillende blinde vlekken waarop aandacht is vereist. Als eerste op het gebied van beleidsvorming, waar gebrek is aan vertaling van gesignaleerde vraagstukken naar beleid en behoefte is aan coherentie en interdepartementale afstemming over digitalisering. Hoe kunnen bestaande verantwoordelijkheden en wet- en regelgeving het best toegepast op de digitale wereld? Waar ontstaan nieuwe verantwoordelijkheden en hoe kunnen die het best worden belegd. Als tweede op het gebied van het politieke debat, waar een structurele discussie over de impact van digitalisering ontbreekt. Als derde en op het gebied van het toezicht, waar behoefte bestaat aan een versterking van het toezicht en aan een betere samenwerking tussen verschillende toezichthouders die op verschillende wijzen met digitalisering te maken.

### **Van incidentenpolitiek naar structurele politiek-bestuurlijke aanpak**

De motie Gerkens vraagt naar de wenselijkheid van een commissie die kan adviseren over de ethische kant van de digitalisering van de samenleving. Wanneer we kijken naar de werking van het governance-ecosysteem rond de maatschappelijke en ethische kant van digitalisering, dan zien we dat op alle verschillende vlakken waar we in het verleden commissies voor hebben gezien (grondrechten, advies, debat, toetsing – zie hoofdstuk 4) actie nodig is.

We zien op verschillende plekken initiatieven waarmee wordt getracht grip te krijgen op nieuwe en opkomende ethische en maatschappelijke kwesties. De discussie dringt op internationaal niveau door in het domein van de mensenrechten. Daar zien we een opkomende discussie over de impact van nieuwe technologieën, zoals AI en robotica, op fundamentele rechten. In Nederland is die discussie buiten de universiteiten nog niet binnen het politiek-bestuurlijke domein geland. Dat geldt tevens voor de maatschappelijke discussie. Het maatschappelijke middenveld in Nederland is voornamelijk georganiseerd rond kwesties als privacy, gegevensbescherming en digitale veiligheid.

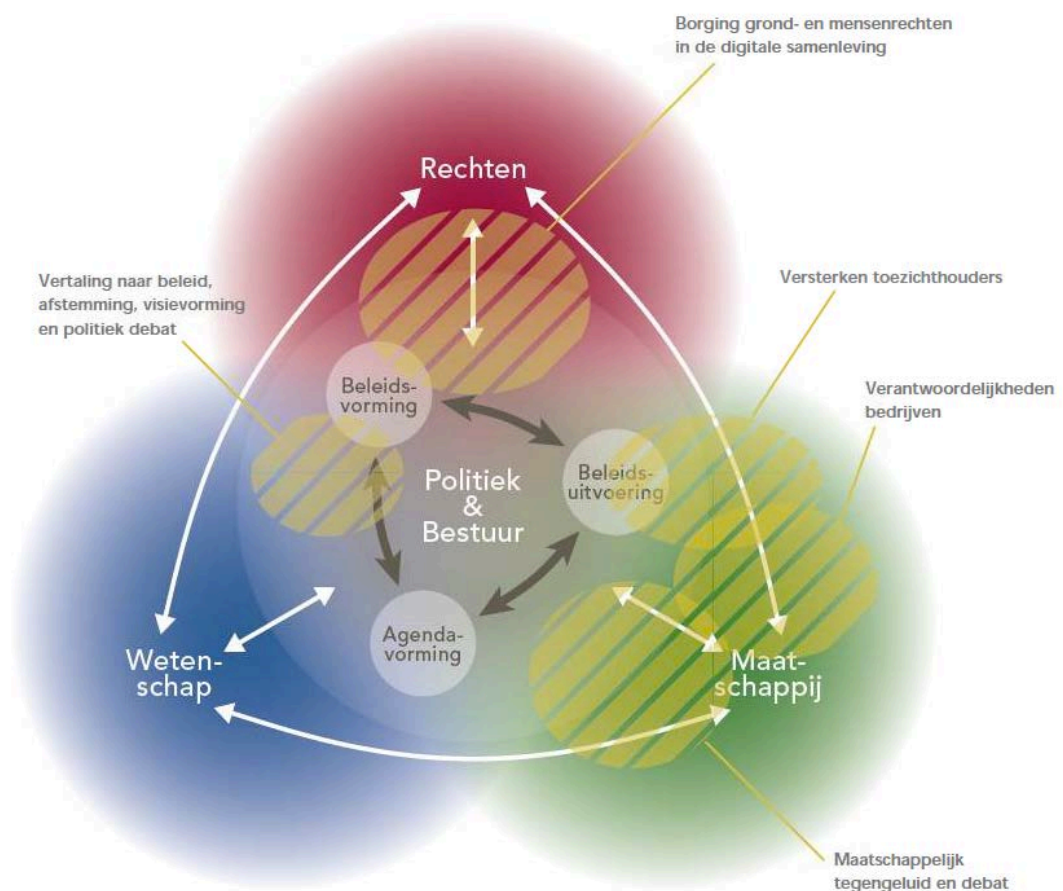
Ons onderzoek laat zien dat in de fase van agendavorming een breed spectrum aan ethische en maatschappelijke kwesties politiek-bestuurlijk op de kaart wordt gezet. De stap naar beleidsvorming en -bepaling vormt echter nog een uitdaging. Het politieke bewustzijn van de impact van digitalisering is aanwezig, maar het debat wordt veel gedreven door incidenten. Tot slot is er de vraag in hoeverre het huidige toetsingsregime nog adequaat is om in het digitale tijdperk belangrijke menselijke waarden en rechten institutioneel te kunnen blijven borgen. Concluderend komen we tot vijf blinde vlekken (zie figuur 5.1):

- De vertaling van nieuwe maatschappelijke en ethische vraagstukken naar beleid, interdepartementale afstemming en coördinatie op digitalisering; en het politieke debat over die nieuwe vraagstukken.
- Borging van grond- en mensenrechten in de digitale samenleving.
- Versterken van toezichthouders en zorgen voor onderlinge afstemming tussen toezichthouders.
- Nieuwe verantwoordelijkheden van ontwikkelaars van digitale diensten en producten.

- Organiseren van maatschappelijk tegengeluid: versterken maatschappelijk middenveld, kennis en vaardigheden van burgers en maatschappelijk debat over digitalisering.

Door deze blinde vlekken in het governancelandschap schiet de bescherming van essentiële publieke waarden in de digitale samenleving momenteel te kort. Er is een structurele aanpak nodig om het governancelandschap op deze 5 plekken substantieel te versterken om zo maatschappelijke en ethische uitdagingen in de digitale samenleving het hoofd te bieden en de Nederlandse burger op adequate wijze te beschermen. In het volgende hoofdstuk zetten we deze aanpak uiteen.

**Figuur 5.1** Blinde vlekken in het governancelandschap



# 6 Conclusie: Borgen van publieke waarden in de digitale samenleving

## 6.1 Inleiding

Op verzoek van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en de Eerste Kamer deed het Rathenau Instituut onderzoek naar de maatschappelijke en ethische kwesties die ontstaan door digitalisering van de samenleving, en naar de wenselijkheid van een commissie die daarover kan adviseren. Dit naar aanleiding van een motie ingediend in de Eerste Kamer van het lid Gerkens (motie Gerkens 23 september 2014, zie kader). De motie verwijst daarbij naar de opkomst van het Internet of Things dat zowel voor kansen als bedreigingen zorgt. Uit de motie blijkt dat bij de Kamer het gevoel leeft dat bij digitalisering belangrijke waarden in het geding zijn, aangezien zij niet alleen spreekt van technologische effecten van digitalisering, maar ook van ‘maatschappelijke, sociaal juridische en sociaal psychologische’ effecten. Voorliggend onderzoek van het Rathenau Instituut ondersteunt die observatie van de Kamer.

### **Kader 6.1 Motie van het lid Gerkens c.s. voorgesteld op 23 september 2014**

De Kamer, gehoord de beraadslagingen, constaterende, dat de digitale technologie met «the Internet of Things» alles en iedereen met elkaar zal verbinden; constaterende, dat deze niet te stuiten ontwikkeling kansen zal bieden voor de maatschappij, maar ook bedreigingen; overwegende, dat de effecten van deze digitale ontwikkeling op de maatschappij niet alleen een technologische, maar ook een maatschappelijke, sociaal juridische en sociaal psychologische is; verzoekt de regering het Rathenau Instituut te vragen een onderzoek te doen naar de wenselijkheid van een commissie die kan adviseren over de ethische kant van de digitalisering van de samenleving, en gaat over tot de orde van de dag.

Ondertekend door Eerste Kamerleden Gerkens, Franken, K.G. de Vries, Strik, Duthler, Van Boxtel.

De motie vraagt naar de wenselijkheid van een commissie die kan adviseren over de ethische aspecten van de digitaliserende samenleving. Die vraag duidt op achterliggende zorgen in de Eerste Kamer of de huidige wettelijke kaders, toezichtsarrangementen en maatschappelijke weerbaarheid nog voldoende zijn om opkomende ethische en maatschappelijke kwesties rond digitalisering het hoofd te bieden. In deze studie hebben we de vraag in de motie vanuit deze achterliggende zorg benaderd. We onderzochten welke technologieën de komende jaren naar verwachting de digitale samenleving vormgeven, en welke maatschappelijke en ethische uitdagingen daardoor ontstaan. Vervolgens hebben we gekeken in hoeverre de omgang met die uitdagingen ook institutioneel verankerd is, oftewel we onderzochten de *governance* van ethische

en maatschappelijke uitdagingen rond digitalisering. Belangrijke deelvragen daarbij waren: hoe is men in het verleden omgegaan met maatschappelijke en ethische kwesties van technologische ontwikkelingen? Hoe krijgt het huidige governancelandschap rond maatschappelijke en ethische digitaliseringsvraagstukken vorm? Welke kwesties pakken Nederlandse instituties en actoren wel of niet op, en op welke manier? Zijn er blinde vlekken waar te nemen? Welke rol kan een commissie spelen? De motie licht niet toe wat voor soort commissie er wordt bedoeld. We hebben in onze analyse daarom ook gekeken naar wat voor soort commissies er in het verleden zijn geweest rond ethische en maatschappelijke kwesties van technologie, en welke rol zij vervulden in het governancelandschap.

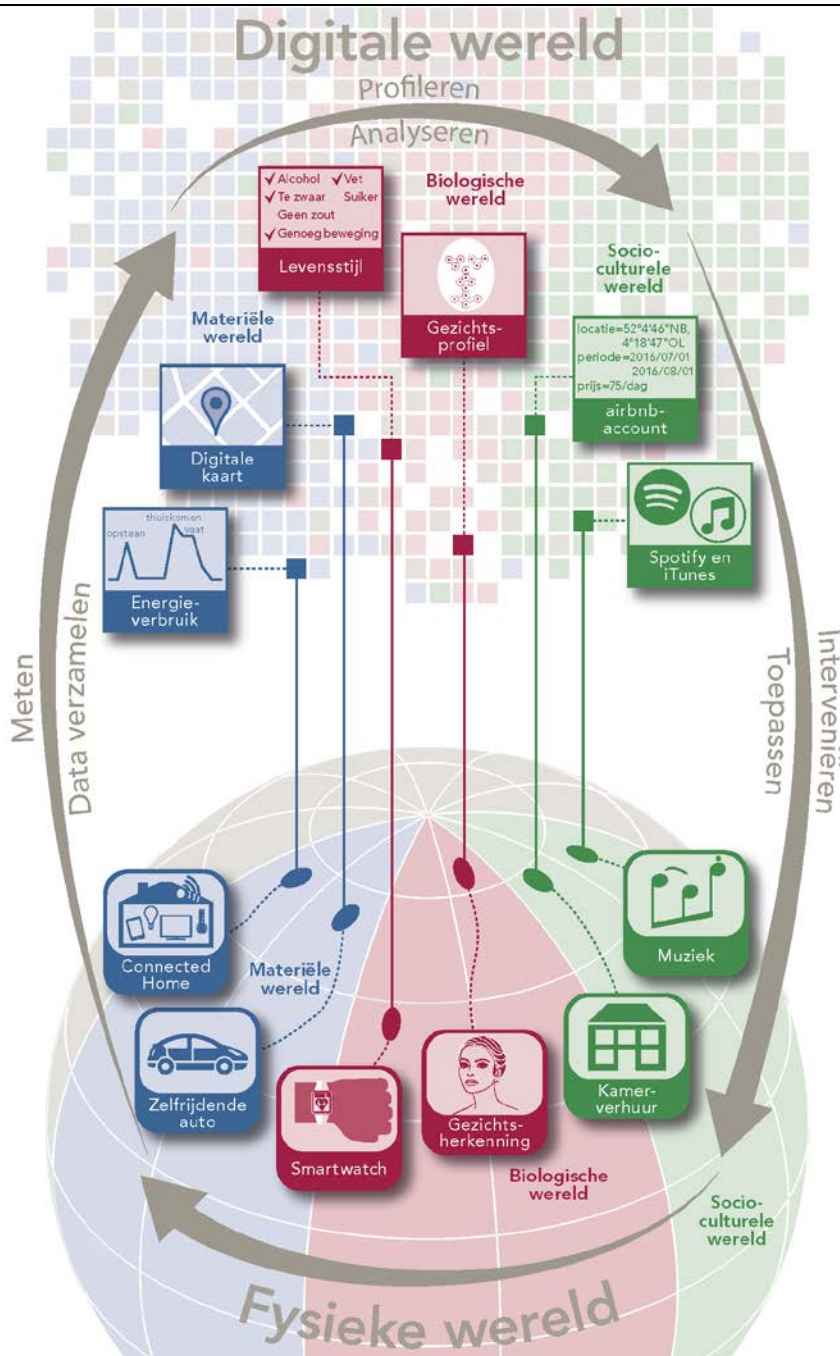
In dit hoofdstuk vatten we eerst de belangrijkste bevindingen uit de studie kort samen. In paragraaf 6.2 bespreken we de technologiegebieden die zorgen voor een nieuwe fase in de digitale samenleving. In paragraaf 6.3 benoemen we de belangrijkste maatschappelijke en ethische uitdagingen die daardoor ontstaan. Vervolgens kijken we in paragraaf 6.4 naar de belangrijkste lessen uit het verleden met betrekking tot het opbouwen van een governancelandschap rond maatschappelijke en ethische kwesties van technologie. In paragraaf 6.5 kijken we waar er blinde vlekken liggen in het governancelandschap dat rond maatschappelijke en ethische digitaliseringsvraagstukken ontstaat. In paragraaf 6.6 komen we op basis daarvan tot acties voor diverse actoren, en beantwoorden we de vraag over de wenselijkheid van een commissie die kan adviseren over de maatschappelijke en ethische kwesties van de digitalisering van de samenleving.

## 6.2 Een nieuwe digitale golf: digitalisering als cybernetisering

De begrippen digitalisering en Internet of Things uit de motie Gerkens refereren aan een groot cluster van digitale technologieën. In hoofdstuk 2 zijn acht technologiegebieden geselecteerd die naar verwachting de digitale samenleving de komende jaren vorm zullen geven: robotica, Internet of Things, biometrie, persuasieve technologie, digitale platformen, augmented reality en virtual reality, kunstmatige intelligentie en big data en algoritmen. Samen zorgen zij voor een nieuwe golf van digitalisering. Steeds meer onderdelen uit de fysieke wereld krijgen een virtuele representatie.

Hoofdstuk 2 liet zien hoe de digitalisering van de biologische, materiële en socio-culturele wereld leidt tot een uitdijende digitale wereld. Er ontstaat een continue terugkoppeling tussen de fysieke en de digitale wereld, waarmee producten of diensten direct worden aangepast op basis van analyse van digitale gegevens (zie figuur 6.1). Denk aan een slimme energiemeter in een *connected home*, dat energieverbruik van de bewoners meet, digitaal analyseert, en vervolgens op basis van dat profiel de thermostaat aanpast. Denk aan de smartwatch, die de activiteiten van de gebruiker bijhoudt en analyseert, en persoonlijke adviezen geeft over de levensstijl van de gebruiker. Of denk aan nieuwe digitale platforms voor kamerverhuur of taxi's, die (in het geval van Uber) continu vraag en aanbod meten en analyseren, om zo met behulp van slimme software dynamisch de prijzen aan te passen, en vraag en aanbod te reguleren.

**Figuur 6.1** Cybernetische loop tussen de fysieke en digitale wereld



Rathenau Instituut

Hoewel digitalisering al decennialang aan de gang is, stellen we in hoofdstuk 2 vast dat we een nieuwe fase van de digitale samenleving inluiden. Deze nieuwe fase kenmerkt zich door een *cybernetische loop* van meten (data verzamelen), profileren (data analyseren) en interveniëren (toepassen van data). Met deze cybernetische loop wordt realtime (bij)sturen in de fysieke wereld mogelijk en ook een steeds centraler uitgangspunt van nieuwe digitale diensten en producten.



De cybernetische *feedback loops* tussen de fysieke en digitale wereld zijn op allerlei terreinen zichtbaar: in het productieproces, de omgeving, het lichaam, en ons gedrag. Het is datasurveillance op het internet, dat gebruikers op basis van het surfgedrag ‘passende’ informatie, nieuwsfeeds, producten of prijzen voorschotelt. Het is de treinfabrikant die via sensoren de prestaties van treintoestellen continue meet en analyseert, en zo bepaalt waar zijn monteurs moeten worden ingezet. Het is de slimme lantaarnpaal op straat, die agressie ‘meet’ en met behulp van licht de sfeer probeert te beïnvloeden. In de publieke sector zien we bijvoorbeeld digitale leerplatformen die leerlingen volgen, en op basis van hun prestaties passende nieuwe opdrachten aanbieden. Of politie-agenten die extra surveilleren op basis van big data-analyses over waar eerder veel inbraken of geweldplegingen zijn gepleegd.

### 6.3 Publieke waarden in het geding

De nieuwe digitaliseringsgolf, en de cybernetische loop die daardoor ontstaat, leiden tot nieuwe maatschappelijke en ethische uitdagingen. Belangrijke publieke waarden zijn hierbij in het geding die nauw verwant zijn aan grond- en mensenrechten. Dat zijn onder andere het recht op gelijke behandeling, privacy, autonomie en menselijke waardigheid (hoofdstuk 3). Hoofdstuk 3 liet ook zien dat de drie processen in de cybernetische loop verschillende maatschappelijke en ethische kwesties oproepen (zie tabel 6.1).

Het proces van dataverzameling en -verwerking – het meten – leidt vooral tot discussies over privacybescherming. Toenemende mogelijkheden om (nieuwe) data te verzamelen en te verwerken bedreigen nieuwe dimensies van privacy. Een voorbeeld is een techniek als emotieherkenning, die leidt tot zorgen over de bescherming van mentale privacy; de vrijheid om te denken en te voelen wat je wilt. De opkomst van het Internet of Things dwingt tot een radicale herziening van ons privacybegrip, bijvoorbeeld ten aanzien van het huis als privé domein en het organiseren van onze fysieke veiligheid. Gerelateerd aan de discussie over privacy, is er ook een discussie over de mogelijkheid tot onafhankelijke identiteitsontwikkeling tot een autonoom individu in een wereld van continue digitale monitoring.

Het proces van data-analyse – het profileren – en de nieuwe technieken die daarvoor worden ingezet zoals zelflerende algoritmen, leiden tot zorgen over bijvoorbeeld het recht op gelijke behandeling en de rol van mensen ten opzichte van computers. Zo speelt software een steeds grotere rol in het maken van beslissingen over mensen. Past iemand in een profiel of niet? Vormt iemand een kredietrisico of niet? Bewust of onbewust kan *data analytics* zorgen voor ongewenste vormen van uitsluiting en discriminatie. Zo blijken softwareprogramma’s die rechters in de Verenigde Staten bijstaan door de kans te berekenen dat een verdachte opnieuw de fout in gaat, in sommige gevallen te discrimineren. Ook kunnen er onjuiste conclusies worden getrokken. Bovendien kan de inzet van data analytics leiden tot een *bias* in de analyse. De inzet van software om te bepalen waar extra politie-inzet nodig is, kan bijvoorbeeld leiden tot een selffulfilling prophecy: daar waar meer politie is, ziet men meer vergrijpen. Die gegevens neemt de computer weer mee in zijn analyse, waardoor het programma verwacht dat er op die locatie meer criminaliteit zal zijn. En doordat technologie menselijke beslissingen overneemt, speelt ook de vraag wat dit betekent voor de autonomie van individuen, en welke mogelijkheden het individu heeft om onjuiste beslissingen van een automatisch systeem recht te zetten.

Bij het proces van terugkoppeling naar de fysieke wereld – het interveniëren en (bij)sturen – ontstaan discussies over hoe ver technologische beïnvloeding mag gaan, hoe autonomie wordt beschermd en wie in welke mate nog controle over technologie heeft. De inzet van robots en software in de zorg, rechtspraak, bankwezen en andere sectoren, stelt bovendien de urgente vraag wat we aan robots willen overlaten, en wat de minimale menselijke betrokkenheid moet zijn om te spreken van bijvoorbeeld betekenisvolle, menswaardige zorg of het kunnen afleggen van betekenisvolle verantwoordelijkheid. Daar komt bij dat publieke diensten in toenemende mate afhankelijk zijn van software die door private partijen ontwikkeld wordt, waardoor het lastig te achterhalen is welke keuzes de software maakt, en welk effect dat heeft. Zal de rechter of dokter in de ene provincie die gebruik maakt van systeem X tot andere uitspraken komen dan een andere rechter of dokter die gebruik maakt van systeem Y?

**Tabel 6.1** Maatschappelijke en ethische vragen in relatie tot de cybernetische loop van digitalisering

	Verzamelen (meten)	Analyseren (profilieren)	Toepassen (intervenieren)
Privacy			
Veiligheid			
Autonomie			
Rechtvaardigheid			
Menselijke waardigheid			
Controle over technologie			
Machtsverhoudingen			

## 6.4 Lessen uit het verleden

In het historische hoofdstuk (hoofdstuk 4) keken we hoe in het verleden is omgegaan met maatschappelijke en ethische aspecten van wetenschap en technologie op vier gebieden: biotechnologie, ICT, mensgebonden onderzoek en dierexperimenten. Dit leidde tot een conceptueel raamwerk van hoe een governance-ecosysteem er op het gebied van wetenschap en technologie uitziet, welke partijen en instituties daar een rol in spelen, en hoe dit ecosysteem zich ontwikkelt. Duidelijk werd dat we om de vraag uit de motie Gerkens te kunnen beantwoorden, (over de wenselijkheid van een commissie die adviseert over de ethische kanten van digitalisering), niet slechts naar een deelaspect van het governance-systeem kunnen kijken, maar dat een breed pallet van governance-activiteiten op het gebied van digitalisering, ethiek en maatschappij relevant is.

Uit de terugblik kwam ook naar voren dat er vaak pas een maatschappelijke discussie ontstaat over de betekenis van nieuwe technologie, als de toepassingen van die technologie breed zichtbaar zijn in de maatschappij, maar dat het dan nog vele, soms zelfs tientallen, jaren duurt om een adequaat governancestelsel op te tuigen. Ook zagen we dat in het verleden diverse typen commissies, met verschillende functies, zijn ingeschakeld om zich te buigen over de governance van ethische en maatschappelijke kwesties rond technologie. Bijvoorbeeld staatscommissies zoals de Commissie Franken die de regering adviseert over aanpassing van de Grondwet, of adviescommissies zoals de Commissie Rathenau of de brede DNA-Commissie die de regering voorziet van advies over een specifieke technologische ontwikkeling, of commissies die zich richten op het organiseren van een maatschappelijke dialoog, zoals de Commissie Maatschappelijke Dialoog Nanotechnologie, of toetsingscommissies die zorgen voor toezicht en toetsing van onderzoek, zoals de Centrale Commissie Mensgebonden Onderzoek, die uitspraken doet over mensgebonden onderzoek en onderzoek met embryo's.

Tot slot maakt het historisch hoofdstuk duidelijk, dat de motie Gerkens aansluit bij een parlementaire traditie om de toekomstbestendigheid van het bestaande governancestelsel voor maatschappelijke en ethische aspecten van technologische ontwikkelingen te bevragen. Het parlement sprak de afgelopen decennia diverse malen over de adequaatheid van de politiek-bestuurlijke omgang met maatschappelijke en ethische kwesties rondom wetenschap en technologie. Dit was vaak naar aanleiding van nieuwe doorbraken in de wetenschap of technologie.

## **6.5 Blinde vlekken in het governancelandschap voor ethische en maatschappelijke digitaliseringsvraagstukken**

In hoofdstuk 5 pasten we het conceptuele raamwerk toe op digitaliseringsvraagstukken. Het bracht in kaart, welke initiatieven en acties er door welke actoren in het governancelandschap worden genomen om met verschillende maatschappelijke en ethische vraagstukken om te gaan. Duidelijk werd dat er op allerlei plekken in het governancelandschap blinde vlekken zijn ontstaan. Met betrekking tot het type maatschappelijke en ethische kwesties dat actoren signaleren en oppakken, zien we een sterke nadruk op initiatieven die samenhangen met de eerste twee processen van de cybernetische loop (meten en profileren). In de afgelopen jaren is de discussie over privacy, gegevensbescherming en online veiligheid uitgegroeid tot het meest in het oog springende maatschappelijke en ethische vraagstuk met betrekking tot digitalisering. Op dit vlak heeft zich in de loop der jaren dan ook een governancestelsel gevormd dat wordt voorzien van wetenschappelijke kennis over de betekenis van nieuwe digitale technologieën op privacy, en waarin beleidsmakers deze kwesties omzetten in beleid, wetten en regelgeving. Er zijn instanties voor toezicht en handhaving, en maatschappelijke organisaties pakken thema's als privacy en veiligheid actief op. Dit governancestelsel is zeker niet uitontwikkeld, zoals de roep om sterker toezicht, Kamervragen om duidelijkere beleidsvisies op privacy, of oproepen tot sterker maatschappelijk debat over het thema laten zien. Actoren in het governancestelsel worden uitgedaagd door nieuwe privacy- en veiligheidsvraagstukken. Belangrijke nieuwe uitdagingen zijn bijvoorbeeld het zoeken naar een digitaal huisrecht, en de bescherming van persoonlijke levenssfeer en veiligheid met de opkomst van het Internet of Things.

Op het gebied van andere maatschappelijke en ethische vraagstukken die samenhangen met ontwikkelingen in AI, robotica en het Internet of Things is het governancestelsel echter nog veel minder uitgekristalliseerd. We zien een groeiende aandacht voor de kwesties rechtvaardigheid en ongelijke machtsverhoudingen. Met betrekking tot rechtvaardigheid komt er aandacht voor algoritmische profilering, de invloed op het recht op gelijke behandeling en de presumpctie van onschuld. Met betrekking tot machtsverhoudingen ontstaat er steeds meer discussie over de machtspositie van grote internetbedrijven. De onderwerpen autonomie, menselijke waardigheid en controle over technologie worden slechts in beperkte mate opgepikt door maatschappelijke organisaties. Deze nieuwe maatschappelijke en ethische kwesties worden wel op wetenschappelijk niveau bestudeerd en aangekaart bij beleidsmakers (voor agendavorming), maar er is nog veel onduidelijk over hoe deze kwesties concreet in beleid moeten worden vertaald. De stap naar beleidsvorming en –bepaling vormt dus nog een uitdaging. Het politieke bewustzijn van de impact van digitalisering is aanwezig, maar het debat wordt veelal gedreven door incidenten. Tot slot werd duidelijk dat het huidige toetsingsregime onvoldoende in staat is om in het digitale tijdperk belangrijke menselijke waarden en rechten institutioneel te kunnen (blijven) borgen.

We zagen dus op vijf onderdelen blinde vlekken in het governancelandschap:

1. De vertaling van nieuwe maatschappelijke en ethische vraagstukken naar beleid, interdepartementale afstemming en coördinatie op digitalisering en het politieke debat over die nieuwe vraagstukken.
2. Borging van grond- en mensenrechten in de digitale samenleving.
3. Versterken van toezichthouders en zorgen voor onderlinge afstemming tussen toezichthouders.
4. Nieuwe verantwoordelijkheden van ontwikkelaars van digitale diensten en producten.
5. Organiseren van maatschappelijk tegengeluid: versterken maatschappelijk middenveld, kennis en vaardigheden van burgers en maatschappelijk debat over digitalisering.

Deze blinde vlekken laten zien dat de bescherming van fundamentele publieke waarden op dit moment sterk tekort schiet. De bescherming van deze essentiële waarden nu en in de toekomst vereist daarom een structurele en geïntegreerde aanpak om de governance van maatschappelijke en ethische kwesties het hoofd te bieden en de Nederlandse burger op adequate wijze te beschermen. Daarbij is het niet altijd nodig om nieuwe regels te ontwikkelen. Digitalisering leidt dikwijls tot conceptuele verwarring over welke regels gelden, en over hoe deze moeten worden toegepast. In sommige gevallen zien we dat bestaande normen, regels en (wettelijke) kaders daardoor (aanvankelijk) niet worden toegepast terwijl deze wel van toepassing zijn. De regulering van de dienst UberPop door de Inspectie Leefomgeving en Transport laat zien dat bestaande kaders ook van toepassing zijn op nieuwe digitale diensten. In andere gevallen zien we dat digitalisering vraagt om nieuwe kaders voor de manier waarop belangrijke waarden worden geborgd in de digitale samenleving. Is er bijvoorbeeld een nieuw grondrecht nodig om betekenisvol menselijk contact te beschermen in een steeds verder digitaliserende zorgomgeving (zie Van Est en Gerritsen, nog te verschijnen)? In de volgende paragraaf beschrijven we welke maatregelen op basis van onze analyse nodig zijn om publieke waarden te borgen in de digitale samenleving.

## 6.6 Opwaarderen: een actieprogramma voor een verantwoorde digitale samenleving

Digitale innovaties ontwikkelen zich razendsnel. Digitalisering dringt door tot in de haarvaten van de samenleving. De voortdurende technische upgrades creëren tal van nieuwe mogelijkheden voor economie en samenleving. Maar het leidt ook tot fundamentele maatschappelijke en ethische vragen. Essentiële publieke waarden komen door de digitalisering van de samenleving onder druk te staan. Alle sectoren van de samenleving krijgen te maken met digitaliseringsvraagstukken en bijbehorende ethische en maatschappelijke uitdagingen. Het is tijd om de fundamentele impact van digitalisering op de samenleving te onderkennen en ervoor te zorgen dat publieke waarden en grondrechten in het digitale tijdperk worden geborgd. Dat vraagt om een upgrade, of opwaardering, van het governancestelsel. Deze opwaardering verwijst naar de benodigde versterking van het governancestelsel, door het structureel borgen van maatschappelijke en ethische waarden.

Deze opwaardering vereist dat alle partijen in de maatschappij in actie komen om digitalisering in goede banen te leiden. Het is onverantwoordelijk om als overheid, bedrijfsleven en als maatschappij van de fundamentele impact van digitalisering weg te kijken. Bij al deze actoren liggen zodoende verantwoordelijkheden om met de maatschappelijke en ethische aspecten van digitalisering om te gaan. Het startschot dient te worden gegeven door de overheid, maar het bedrijfsleven en het maatschappelijk middenveld behoren tegelijkertijd stappen te ondernemen.

Onze centrale conclusie is dan ook dat de Eerste Kamer **terecht haar zorgen uit over de ethische en maatschappelijke impact van digitalisering** in de motie Gerkens. De Eerste Kamer vraagt zich daarbij af in hoeverre het wenselijk is om een commissie in te stellen die kan adviseren over de ethische kanten van de digitale samenleving. Onze analyse laat zien dat **om essentiële publieke waarden te borgen, het governancestelsel op het terrein van de maatschappelijke en ethische aspecten van digitalisering op meerdere plekken substantieel dient te worden versterkt.**

Het instellen van een commissie voldoet niet aan de geconstateerde problemen in onze analyse. In de jaren '70 en '80 werd het bestuderen van maatschappelijke en ethische kwesties rond nieuwe technologie overgelaten aan enkele wetenschappelijke experts in commissies. In de jaren '90 kwam er meer oog voor de wensen en zorgen van burgers over deze kwesties. Ingestelde commissies werden breder van samenstelling om zo een beter maatschappelijk debat te kunnen voeren. Tegenwoordig vraagt de aanpak van complexe problemen om de gezamenlijke inzet van meerdere actoren. Na overeenstemming over het doel (bijvoorbeeld het verminderen van CO<sub>2</sub>-uitstoot), ligt de grootste uitdaging in de vraag, hoe partijen samen het beste uitvoering kunnen geven aan dat doel. Op het gebied van energie is tegen deze achtergrond bijvoorbeeld door meer dan veertig partijen een 'Energieakkoord' afgesloten om zich in te zetten voor een besparing van het energieverbruik.

Een commissie alleen kan de blinde vlekken in het governancestelsel niet oplossen. Een complex probleem als de versterking van het governancestelsel vraagt dat alle partijen hun verantwoordelijkheid nemen, en zich gezamenlijk inzetten voor de borging van publieke waarden in de digitale samenleving. Met het instellen van een commissie bestaat tevens het risico dat

problemen in de praktijk bij de commissie worden 'geparkeerd' en partijen in het veld en op politiek-bestuurlijk niveau een (te) afwachtende houding aannemen. Bovendien heeft voorliggende studie het voorwerk van een dergelijke commissie reeds uitgevoerd. De studie brengt in kaart, welke maatschappelijke en ethische digitaliseringsvraagstukken op ons afkomen, en waar in het governancelandschap om die vraagstukken het hoofd te bieden blinde vlekken liggen. Zij biedt tevens handelingsperspectieven voor alle betrokken partijen om het governancelandschap te versterken.

**De belangrijkste boodschap van het Rathenau Instituut is dat de overheid, het bedrijfsleven en het maatschappelijk middenveld nu actie dienen te ondernemen om het governancelandschap te versterken en zo publieke waarden in de digitale samenleving te kunnen blijven borgen.**

We stellen een vijftal acties voor waarmee beleidsmakers, bedrijven en maatschappelijke organisaties het governancelandschap verantwoord kunnen opwaarderen:

1. Stel een interdepartementale werkgroep in die toewerkt naar een kabinetsvisie op de omgang met de maatschappelijke en ethische betekenis van digitalisering, en die zorgt voor politiek-bestuurlijke coördinatie.
2. Versterk de rol en positie van toezichhouders.
3. Stel een "Digitaliseringsakkoord" op om commitment en verantwoordelijkheden van bedrijven, overheid, en maatschappelijke actoren omtrent de borging van publieke waarden in de digitale samenleving vast te leggen.
4. Organiseer een nationale dialoog over de betekenis van digitalisering voor de borging van publieke waarden.
5. Zorg voor periodieke politieke discussie in de Eerste en Tweede Kamer over de governance van maatschappelijke en ethische digitaliseringsvraagstukken.

Elke actie valt uiteen in een aantal specifieke actiepunten, die we hieronder toelichten.

### **1. Stel een interdepartementale werkgroep in die toewerkt naar een kabinetsvisie op de omgang met maatschappelijke en ethische betekenis van digitalisering.**

Actiepunten voor de interdepartementale werkgroep:

- Zorg voor coördinatie van en overkoepelende visievorming op de maatschappelijke en ethische impact van digitalisering en de borging van publieke belangen.
- Verken hoe grondrechten in het digitale tijdperk kunnen worden geborgd. Hierbij is van belang om verbinding te zoeken met en oog te houden voor initiatieven op Europees niveau, bijvoorbeeld bij de Raad van Europa.

### **Coördinatie en visievorming**

De vertaling van de gesignaleerde ethische en maatschappelijke vraagstukken naar een coherent en domeinoverstijgend beleid verloopt moeizaam. Om het gefragmenteerde karakter van de discussie te ontstijgen, is er op politiek-bestuurlijk niveau behoefte aan een overkoepelende kabinetsvisie. Een interdepartementale werkgroep is nodig om toe te werken naar een kabinetsvisie op de governance van maatschappelijke en ethische digitaliseringsvraagstukken, en deze op

integrale en strategische wijze binnen de overheid te beleggen. De werkgroep kan de verschillende beleidsvragen van ministeries coördineren en afstemmen, en zo zorgen voor coherentie in de vraagstukken die beleidsoverstijgend zijn. De werkgroep kan er ook voor zorgen dat het besef van de betekenis van digitalisering voor de borging van publieke waarden groeit binnen de overheid, en verschillende ministeriële departementen stimuleren de betekenis van nieuwe maatschappelijke en ethische vragen op hun terrein te doordenken en te adresseren.

### **Borging van grondrechten**

Er ligt in het politiek-bestuurlijke domein een verantwoordelijkheid om de betekenis van digitalisering voor de borging van grondrechten te monitoren. Discussies over de impact van digitalisering op de bescherming van fundamentele rechten hebben zich in Nederland nog voornamelijk geconcentreerd op of en hoe het recht op privacy, vertrouwelijke communicatie en de vrijheid van meningsuiting aangepast zouden moeten worden in het licht van digitalisering. Recent zijn er initiatieven op Europees niveau gekomen (bijvoorbeeld bij de Raad van Europa, maar ook bij het Europees Parlement) die onderzoeken wat de opkomst van technologieën als big data, AI, robotica, en het Internet of Things betekenen voor de bescherming van fundamentele rechten. Hoe kunnen die blijvend worden geborgd in het digitale tijdperk? Voor biotechnologie en gentechnologie is bijvoorbeeld in 1997 op initiatief van de Raad van Europa een apart verdrag opgesteld (Verdrag van Oviedo). Ondanks het brede toepassingsbereik van het Europees Verdrag voor de Rechten van de Mens (EVRM), achtte de Raad van Europa het noodzakelijk om zich expliciet te richten tot nieuwe wetenschappelijke en technologische ontwikkelingen; er moest een balans tussen vooruitgang en menselijke waardigheid worden gezocht. Nu speelt de vraag of er een vergelijkbaar verdrag nodig is voor de bescherming van grondrechten met betrekking tot de nieuwe golf van digitalisering (Van Est & Gerritsen nog te verschijnen).<sup>93</sup> Ook Nederland dient de betekenis van digitalisering op grondrechten te verkennen en kennis te nemen van, (en verbinding te zoeken met), de Europese initiatieven op dit gebied. Ook hier ligt een taak voor de interdepartementale werkgroep.

## **2. Versterk rol en positie toezichhouders**

### Actiepunten

- Toezichhouders: neem kennis van nieuwe maatschappelijke en ethische vraagstukken.
- Toezichhouders: verken hoe vanuit het huidige mandaat invulling gegeven kan worden aan deze nieuwe vraagstukken: welke regels zijn van toepassing, welke instrumenten hebben toezichhouders tot hun beschikking, welke capaciteit/kennis is nodig?
- Toezichhouders: stem in gezamenlijk overleg af wie waar verantwoordelijk voor is, en treedt waar nodig gezamenlijk op.
- Overheid: bouw voorwaarden in & vervul de rol van launching customer.

---

<sup>93</sup> De Parlementaire Assemblee (PACE) van de Raad van Europa onderzoekt hoe convergerende technologieën, artificiële intelligentie en robotica mensenrechten beïnvloeden en hoe deze in het digitale tijdperk beschermd kunnen worden. Zie ook: Technological convergence, artificial intelligence and human rights. Motion for a resolution. Doc. 13833, 24 June 2015. Parliamentary Assembly of the Council of Europe. [assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21951&lang=en](http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21951&lang=en). In juni 2016 is het Rathenau Instituut door PACE gevraagd om een expertpaper te schrijven over hoe technologische convergentie, kunstmatige intelligentie en robotica mensenrechten beïnvloeden.

Alle toezichthouders krijgen te maken met nieuwe digitaliseringsvraagstukken, of het nu gaat om kwesties als privacy, discriminatie, machtsverhoudingen of menselijke waardigheid. Alle toezichthouders, zoals de Autoriteit Persoonsgegevens, de Autoriteit Consument en Markt, het College voor de Rechten voor de Mens, Inspectie Leefomgeving en Transport of de Nationale Zorgautoriteit, dienen zich te oriënteren op de vraag hoe zij op hun terrein praktisch, vanuit hun huidige mandaat, invulling kunnen geven aan nieuwe ethische en maatschappelijke digitaliseringsvraagstukken. Daarbij is onderlinge afstemming van groot belang. Doordat digitalisering verschillende sectoren doorkruist zal het handavingsdomein van verschillende toezichthouders regelmatig overlappen. Toezichthouders dienen daarom overleg te voeren over de manier waarop zij worden geconfronteerd met digitalisering, hoe het toezicht wordt georganiseerd en waar verantwoordelijkheden van verschillende toezichthouders liggen.

Rondom privacy en gegevensbescherming heeft zich bijvoorbeeld een duidelijke rol afgetekend voor de Autoriteit Persoonsgegevens en de Autoriteit Consument en Markt. Toch krijgen ook zij met nieuwe vraagstukken te maken. In Europa onderzoekt bijvoorbeeld de Europese Data Protectie Supervisor (de Europese toezichthouder op het gebied van persoonsgegevens) haar rol op het vlak van ethische digitaliseringsvraagstukken. Ze kijkt daarbij zowel inhoudelijk naar welke nieuwe kwesties ontstaan, als naar hoe zij vanuit haar huidige mandaat deze nieuwe kwesties kan oppakken.

Voor vraagstukken rondom discriminatie door software, de inzet van software en robots en het behoud van menselijke waardigheid, en het ontstaan van nieuwe machtsverhoudingen tussen consument, bedrijf en overheden, zijn de rollen voor toezichthouders veel minder scherp afgetekend. Wie houdt er bijvoorbeeld toezicht op de mogelijk discriminerende uitwerking van softwareprogramma's? Wie signaleert dat softwareprogramma's van verschillende fabrikanten mogelijk verschillende adviezen geven over kans op recidive, of over diagnose van ziektes?

Het oriënteren op digitale vraagstukken wil niet per se zeggen dat er een nieuwe toezichthouder of nieuwe wet- en regelgeving nodig is. Vaak biedt bestaande wet- en regelgeving al een kader, zoals de Algemene Verordening Gegevensbescherming een kader biedt om automatische beslissingen door algoritmen onder de loep te nemen. Soms zullen het huidige mandaat en de instrumenten die een toezichthouder heeft voldoende zijn, soms zal aanpassing nodig zijn.

Bij het versterken van de positie van de toezichthouders dient men bovendien voor ogen te houden dat het niet alleen draait om het kennismaken van nieuwe vraagstukken en capaciteit opbouwen om deze vraagstukken op te pakken, maar ook om de vraag of de randvoorwaarden voldoende aanwezig zijn om dat te kunnen doen. De overheid kan normerende kaders opstellen waaraan de aanschaf, ontwerp en inrichting van systemen moeten voldoen, en waar toezichthouders en handhavers op kunnen toetsen. Bijvoorbeeld door vast te stellen hoe een software-ontwikkelaar verantwoording kan afleggen over de werkwijze van complexe algoritmen, zodat software-ontwikkelaars dat in het ontwerp van het systeem inbouwen. Op deze manier wordt duidelijk welke systemen, in welke situaties, aan bepaalde transparantievoorwaarden moeten voldoen. Dat speelt nog sterker wanneer het gaat om (semi)publieke diensten en digitale systemen in de zorg, het onderwijs, het rechtssysteem en dergelijke. De overheid dient daar op te treden rol als hoeder van publieke belangen. Door toenemende *servitization* (waarbij producten als diensten worden



aangeboden, zie hoofdstuk 3) zijn systemen van publieke diensten steeds vaker in handen van private partijen, waardoor overheid, toezichthouders en handhavers vaak onvoldoende zicht hebben op de werking en effecten van deze systemen en onvoldoende mogelijkheden om controle uit te oefenen. Het moet mogelijk zijn om de inrichting van het systeem en de uitwerking daarvan te kunnen controleren. De overheid dient zich hiervan bewust te zijn bij de aanbesteding van digitale systemen en hiertoe van tevoren voorwaarden voor op te stellen.

### **3. Stel een “Digitaliseringsakkoord” op om commitment en verantwoordelijkheden van bedrijven, overheid, en maatschappelijke actoren omtrent de borging van publieke waarden in de digitale samenleving vast te leggen.**

Actiepunten voor het Digitaliseringsakkoord:

- Bedrijven: zet de zorgplicht centraal om rekening te houden met maatschappelijke en ethische vraagstukken van digitale producten en diensten.
- Bedrijven en brancheorganisaties: zorg voor praktische invulling van de zorgplicht via gedragscodes.
- Bedrijven, brancheorganisaties en wetenschap: verken en leer van bestaande tools en structuren die het bedrijfsleven kunnen helpen om met ethische impact om te gaan. Privacy impact assessments kunnen als voorbeeld dienen voor een ethical impact assessment.
- Overheid en wetenschap: investeer via onderzoeksfinanciering en innovatiebeleid in verkenning en aanpak van maatschappelijke en ethische implicaties van nieuwe technologie.
- Overheid: onderzoek hoe tegengeluid van niet-gouvernementele organisaties en burgers kan worden versterkt (bijvoorbeeld met class actions, en door te onderzoeken in hoeverre het wenselijk is het verbod grondwettelijke toetsing op te heffen).
- Overheid, bedrijven en maatschappelijk middenveld: zet meer in op digitale vaardigheden in het onderwijs (aan jongeren en professionals).
- Overheid, bedrijven en maatschappelijk middenveld: verbreed mediawijsheid (inzicht in werking nieuwe technologie).

In samenwerking met de overheid zullen het bedrijfsleven, het maatschappelijk middenveld en burgers tevens stappen moeten ondernemen om publieke waarden in de digitale samenleving, nu en in de toekomst, te kunnen borgen. Het verdient daarom aanbeveling dat betrokken partijen – bedrijven, maatschappelijk middenveld en overheid – gezamenlijk een “Digitaliseringsakkoord” opstellen. In dit akkoord kunnen partijen hun verantwoordelijkheden vastleggen om samen te werken aan een ‘humaan gezicht’ van de digitale samenleving. Voor het opstellen van een Digitaliseringsakkoord is het van belang dat er draagvlak is bij bedrijven en deelnemende stakeholders. Voor het proces kan er gekeken worden naar de aanpak die is gevolgd bij de totstandkoming van eerdere akkoorden, zoals het Energieakkoord.

#### *Belang van een “Digitaliseringsakkoord”*

Het realiseren én uitvoeren van een dergelijk akkoord is van cruciaal belang voor Nederland. Maatschappelijke en ethische kwesties worden, net als bij biotechnologie, belangrijke succes- en faalfactoren voor innovatie. Het niet tijdig inspelen op het beschermen van publieke waarden, kan het vertrouwen van consumenten en burgers schaden en leiden tot falende innovaties en kostbare trajecten. Een voorbeeld is de slimme meter, waarbij de Eerste Kamer twee wetten om deze in te

voeren blokkeerde (onder andere vanwege privacyzorgen), waardoor de introductie van de apparaten significante vertraging opliep (Cuijpers en Koops 2012). Met het op een juiste manier borgen van publieke waarden in toekomstige ICT-innovaties, kan Nederland een gidsland worden en kansen creëren voor het Nederlandse bedrijfsleven.

Op verschillende plekken zien we recent samenwerkingen en aanzetten van partijen om serieus werk te maken van 'de digitale samenleving'. De diverse oproepen hebben gemeen dat ze benadrukken om op een verantwoorde manier in te zetten op digitalisering, om Nederland een unieke kans te geven om voorop te lopen. Ze signaleren versnippering in het huidige digitaliseringsbeleid vanuit de overheid, en roepen de overheid op om meer regie te voeren. Het ontwikkelen van digitale vaardigheden komt ook in meerdere oproepen terug. Tegelijkertijd zijn bij de bestaande oproepen of een deel van de benodigde partijen vertegenwoordigd, of wordt slechts voor een beperkt deel van de maatschappelijke en ethische digitaliseringsvraagstukken aandacht gevraagd. Een voorbeeld is het 'Manifest: samen naar een duurzame digitale samenleving' ondertekend door 27 partijen (bedrijfsleven, kennisinstellingen en koepelorganisaties) tijdens het Jaarcongres van ECP op 17 november 2016 (VNO-NCW 2016). Het manifest vraagt aandacht voor het belang van duurzame digitalisering van de samenleving en roept o.a. op tot aandacht voor zorgen als werkgelegenheid, cyberweerbaarheid en privacy. In dit manifest is echter nog geen structurele aandacht voor de 'nieuwe' maatschappelijke en ethische digitaliseringsvraagstukken, zoals gelijke behandeling, menselijke waardigheid en autonomie. Daarnaast zijn de ondertekenaars voornamelijk partijen en (koepel)organisaties uit het bedrijfsleven of de wetenschap, en zit er slechts één organisatie bij die de belangen van de burger vertegenwoordigt. Andere oproepen komen uit een specifieke hoek. Zo roepen bijvoorbeeld de werkgeverskoepel VNO-NCW, MKB-Nederland en LTO-Nederland op tot een 'digitale kwantumsprong' voor Nederland: het beter benutten van de kansen van digitalisering, door regelgeving publieke belangen blijven waarborgen (NL next level 2016). Bij de publieke belangen gaat het ook hier om werkgelegenheid, privacy en veiligheid, nog niet om de ethische en maatschappelijke effecten in de volle breedte. Een andere oproep komt vanuit de wetenschap, waarbij de Vereniging van Universiteiten (VSNU) aangeeft dat zij de komende jaren zal inzetten op 'mensgerichte informatietechnologie', waarbij ook hier privacy en veiligheid met name worden genoemd.

Vele partijen lijken dus doordrongen van het belang om op een verantwoorde manier de vruchten te plukken van digitalisering, en zijn bereid daarvoor de handen ineen te slaan. De uitdaging ligt dan ook in uitbreiding van de bestaande initiatieven naar niet alleen een oproep tot de bescherming van privacy en zorg voor online veiligheid, maar naar de bescherming van alle grondrechten en publieke waarden die door digitalisering worden geraakt. Naast deze inhoudelijke verbreding, is ook een verbreding van het aantal organisaties uit het maatschappelijk middenveld van belang, met name een sterkere vertegenwoordiging door organisaties die de belangen van burgers behartigen.

#### *Actiepunten in het Digitaliseringsakkoord*

In een "Digitaliseringsakkoord" dienen verantwoordelijkheden van verschillende partijen te worden gedefinieerd en vastgelegd. Een belangrijk onderdeel van een dergelijk akkoord vormen de verantwoordelijkheden van bedrijven. ICT-producten en diensten zijn inmiddels geen *gadgets* meer: ze hebben een fundamentele impact op onze maatschappij en raken grond- en mensenrechten. ICT-ontwikkelaars dienen doordrongen te zijn van de maatschappelijke en ethische impact van hun

producten, en dienen zich in te spannen voor de bescherming van mensenrechten en grondrechten. De verantwoordelijkheid van bedrijven om mensenrechten te respecteren zijn onder andere opgenomen in de Richtlijnen voor Multinationale Ondernemingen van de OESO. Bedrijven dienen zich actief in te spannen om risico's op schendingen van mensenrechten door henzelf of partijen in hun keten te onderkennen, en waar mogelijk schendingen te voorkomen.

Via gedragscodes van brancheorganisaties kan praktische uitwerking worden gegeven aan deze internationale standaarden. Ze geven richting aan de omgang met maatschappelijke en ethische vragen. Leer van bestaande structuren en tools op het gebied van dataprotectie, zoals privacy impact assessments en privacy by design. Zo kan een *ethical impact assessment* bijvoorbeeld een middel zijn om maatschappelijke en ethische knelpunten anders dan privacy in een vroege fase van productontwikkeling zichtbaar te maken. De overheid kan hier een rol spelen door in haar onderzoeksfinanciering en innovatiebeleid nadrukkelijk ruimte te maken voor maatschappelijke en ethische implicaties van nieuwe technologie (Hessels en Deuten, 2012).

Daarnaast dient het Digitaliseringsakkoord aandacht te besteden aan het stimuleren van digitale vaardigheden. Dat kan concreet vorm krijgen door in het onderwijs mediawijsheid te verbreden, en ruimte te maken voor programmeren en andere digitale vaardigheden. Dat geldt niet alleen voor het basis- en voorgezet onderwijs voor de burgers van de toekomst, maar juist ook voor het onderwijs van de professionals van nu. Van de zorg tot aan het gerechtelijke systeem is het van belang dat professionals kennis nemen van de invloed van de nieuwe digitaliseringsgolf op publieke waarden.

Tot slot is het van belang dat het akkoord vastlegt hoe het tegengeluid van niet-gouvernementele organisaties (ngo's) en burgers beter kan worden ondersteund, bijvoorbeeld door zogenaamde class actions, of door de wenselijkheid van het opheffen van het verbod op grondwettelijke toetsing te onderzoeken.

#### **4. Versterken technologisch burgerschap middels een maatschappelijke dialoog**

Actiepunten:

- Overheid, bedrijven en maatschappelijk middenveld: ondersteun technologisch burgerschap door een nationale dialoog over nieuwe maatschappelijke en ethische digitaliseringsvraagstukken te organiseren.

De maatschappelijke discussie over de maatschappelijke en ethische betekenis van de nieuwe digitaliseringsgolf is vooralsnog beperkt, met name over de nieuwe vraagstukken als gelijke behandeling, menselijke waardigheid, autonomie en nieuwe machtsverhoudingen tussen bedrijven en consumenten, bedrijven en overheden, en tussen burgers en overheden. Dat betekent dat er een belangrijke taak ligt in het organiseren van een nationale dialoog over deze ontwikkelingen. De overheid dient hiertoe het startschot te geven, maar een maatschappelijk dialoog kan alleen succesvol zijn in samenwerking met het veld. De uitvoerende verantwoordelijkheid voor het organiseren van de dialoog zal niet bij de overheid liggen, maar zij is wel de initiator en aanjager. Er kan gebruik worden gemaakt van de ervaring die is opgedaan met de organisatie van eerdere dialogen zoals de maatschappelijke dialoog nanotechnologie.

De dialoog vormt samen met het stimuleren van digitale vaardigheden (zie hierboven) de kern van technologisch burgerschap. Technologisch burgerschap houdt in dat burgers zich bewust zijn van de technologische cultuur waarin ze leven, en begrijpen op welke manier technologie invloed op hen uitoefent (Van Est 2016). Een 'technologisch burger' is geïnformeerd over de werking van technologie, kan kritisch nadenken over die werking en de betekenis daarvan voor zijn leefwereld, en kan op basis daarvan kiezen welke technologie hij wel of niet kan of wil gebruiken. Dat betekent bijvoorbeeld dat mensen begrijpen hoe profilering en zelflerende algoritmes werken en hoe dat hen beïnvloedt, en dat ze in staat zijn zich te verweren tegen ongewenste invloeden, en alternatieven kunnen kiezen. Technologisch burgerschap vraagt daarom om het vergroten van het maatschappelijk bewustzijn en het stimuleren van de meningsvorming over de invloed en betekenis van de nieuwe digitaliseringsgolf.

### **5. Zorg voor periodieke politieke discussie in de Eerste en Tweede Kamer over de governance van maatschappelijke en ethische digitaliseringsvraagstukken**

Actiepunten:

- Periodieke discussie over de governance van maatschappelijke en ethische digitaliseringsvraagstukken.

Een overkoepelende kabinetsvisie op de omgang met de maatschappelijke en ethische betekenis van digitalisering brengt met zich mee dat het onderwerp ook periodiek op de politieke agenda komt te staan. Daarmee wordt invulling gegeven aan de geconstateerde behoefte in het parlement aan een structurele discussie over maatschappelijke en ethische digitaliseringsvraagstukken. Die behoefte blijkt uit oproepen vanuit het parlement, waarbij de Eerste en Tweede Kamer de regering regelmatig verzoeken om een integrale visie te vormen op gebieden als privacy, of de rol van ethiek in innovatiebeleid. De motie Gerkens (zie kader 6.1) en de motie Ester c.s. (Kamerstukken I, 2013-2014, 33750 XIII) zijn daar voorbeelden van. Motie Ester verzoekt het Ministerie van Economische Zaken om jaarlijks te rapporteren over de rol van ethiek in het innovatiebeleid, en probeert daarover een structureel terugkerende politiek-ethisch debat in de Eerste Kamer mogelijk te maken. Tot nu toe wordt het politieke debat met name gedreven door incidenten. Door het onderwerp periodiek (liefst commissieoverstijgend) op de Kameragenda te zetten ontstaat het debat het huidige gefragmentariseerde en incidentele karakter, en kan worden bezien of de ondernomen acties om het governance-landschap te versterken daadwerkelijk vruchten hebben afgeworpen: is het landschap voldoende versterkt? Zijn er nieuwe blinde vlekken ontstaan? En zijn er aanvullende acties gewenst?

## **6.7 Tot slot**

De digitalisering van de samenleving gaat een nieuwe fase in. Voor allerlei essentiële diensten en producten maken we in toenemende gebruik van digitale technologieën en zijn we steeds afhankelijker van digitale systemen: in de zorg, het bankwezen, de media, het onderwijs of de rechterlijke macht. De opkomst van het Internet of Things laat het onderscheid tussen online en offline vervallen: we zijn onlife. Big data en algoritmen ondersteunen beslissingen in de publieke en private sectoren, van het opsporen van fraude, kansen op recidive, tot aan hulp bij het stellen van

medische diagnoses. In sommige gebieden neemt software al beslissingen van mensen over, bijvoorbeeld bij de inzet van bewapende drones, of bij slimme auto's op de weg. Persuasieve technologie, ingebed in adviserende apps op onze smartphone of in slimme lantaarnpalen, beïnvloeden ons gedrag en autonomie op subtiële wijze.

Deze studie laat zien dat publieke waarden door deze nieuwe digitaliseringsgolf onder druk staan. ICT-diensten en producten zijn geen *gadgets* meer: ze hebben een fundamentele impact op onze maatschappij. Het is tijd om die fundamentele impact te onderkennen en ervoor te zorgen dat publieke waarden en grondrechten in het nieuwe digitale tijdperk geborgd zijn. Daarbij is het van belang om op te merken dat technologie op zichzelf nooit goed of slecht is, of neutraal (Kranzberg 1986). Technologie kan diverse maatschappelijke en ethische implicaties hebben, maar deze variëren sterk naar gelang de context en praktijken waarin de technologie wordt ingezet, en hoe deze ontworpen is. De bouwblokken en de infrastructuur van de nieuwe digitale samenleving krijgen nu hun beslag. Maar het governancestelsel om om te gaan met de maatschappelijke en ethische kwesties daardoor ontstaan, schiet op meerdere dimensies tekort, zo blijkt uit deze studie. Rollen en verantwoordelijkheden zijn op meerdere terreinen onduidelijk geworden. Maatschappelijke en ethische kwesties worden wel geagendeerd maar niet vertaald naar beleid om publieke waarden in de praktijk te beschermen. Toezichthouders hebben onvoldoende zicht op nieuwe digitaliseringsvraagstukken. Maatschappelijke organisaties en burgers hebben te weinig zicht op de nieuwe digitale ontwikkelingen en hoe dat hen raakt, en te weinig mogelijkheden om zich daartoe te verweren.

Tegelijkertijd is duidelijk dat we niet met lege handen staan. Bestaande normen, regels en wetten zijn vaak ook van toepassing in de onlife wereld. Het belang van de bescherming van publieke waarden en grondrechten is alom erkend; ze zijn vastgelegd in o.a. de Nederlandse Grondwet, het EU-Handvest van de Grondrechten en door Nederland geratificeerde internationale verdragen, zoals de Universele Verklaring van de Rechten van de Mens van de Verenigde Naties (1948). De belangrijkste taak die voor ons ligt, is dan ook om alom erkende publieke waarden in de alledaagse praktijk van de nieuwe digitale samenleving daadwerkelijk te borgen. Zonder actie van overheid, bedrijfsleven, maatschappelijk middenveld en burgers bestaat het gevaar dat terwijl we grip proberen te krijgen die nieuwe digitale wereld, de kaders voor de bescherming van publieke waarden in de praktijk aan betekenis verliezen.

# Bibliografie

Acquisti, A., R. Gross & F. Stutzman (2014). Face recognition and privacy in the age of augmented reality. In: *Journal of Privacy and Confidentiality* 6(2), Article 1.

AIV (2014) Het Internet. Een wereldwijde vrije ruimte met begrensde staatsmacht. No. 92. Den Haag: Adviesraad Internationale Vraagstukken.

Andorno, J. (2006) Global bioethics at UNESCO: In defence of the Universal Declaration on Bioethics and Human Rights. In: *J Med Ethics* 33(3), pp. 150–154.

Andrade, N. (2014) Computers are getting better than humans at facial recognition. In: *The Atlantic*, 09-06-2014.

Anthes, G. (2006) Bits to Atoms (and Atoms to Bits). In: *Computerworld*, 03-04-2006.

AP (2016) *AP Agenda 2016*. Den Haag: Autoriteit Persoonsgegevens.

Arkin, R. (2010) The Case for Ethical Autonomy in Unmanned Systems. In: *Journal of Military Ethics*, Vol. 9, Issue 4, pp. 332-341.

Barby, E. (2012) The internet of things, legal Aspects: What will change (everything)... In: *Communications & Strategies* 87(3), pp. 83-100.

Benkler, Y. (2006) *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven: Yale University Press.

Bogaard, van den A., H. Lintsen, F. Veraart & O. de Wit (red.) (2008) *De eeuw van de computer: de geschiedenis van de informatietechnologie in Nederland*. Deventer: Kluwer – Stichting Historie der Techniek.

Borenstein, J. & Y. Pearson (2010). Robot caregivers: harbingers of expanded freedom for all? In: *Ethics and Information Technology* 12(3), pp. 277-288.

Boxsel, van, J.A.M. (red.) (1991) *Ethische aspecten van wetenschap en technologie*. Den Haag: NOTA.

Boyd, D. (2014) *It's Complicated: The Social Lives of Networked Teens*. New Haven, CT: Yale University Press.

Bresnahan, T.F. & M. Trajtenberg (1995) General Purpose Technologies. Engines of Growth? In: *Journal of Econometrics* 65, pp. 83-108.

Brinkman, B. (2015). Ethics and pervasive augmented reality: Some challenges and approaches. In: K.D. Pimple (red.), *Emerging Pervasive Information and Communication Technologies*, Dordrecht: Springer, pp. 149-175.

Bronstein, J., Tagliati, M., Alterman, R.L., Lozano, A.M., Volkmann, J., Stefani, A. et al. (2012) Deep Brain Stimulation for Parkinson Disease. An Expert Consensus and Review of Key Issues. In: *JAMA Neurology* 68(2).

Brynjolfsson, E. & A. McAfee (2014). *The Second Machine Age. Work, Progress, and Prosperity in a Time of Brilliant Technologies*. New York: WW Norton.

BSI (2016) Robots and robotic devices. Guide to the ethical design and application of robots and robotic systems. BS 8611:2016. London: BSI.

Burkeman, O. (2014) Can I increase my brain power? In: *The Guardian*, 04-01-2014.

Carr, N. (2010) *The Shallows. What the Internet Is Doing to Our Brains*. New York: W.W. Norton.

Castells, M. (1996) *The Rise of the Network Society. The Information Age: Economy, society and culture* 1. Cambridge, MA: Blackwell Publishing Ltd.

Cate, F., P. Cullen & V. Mayer-Schönberger (2014). *Data Protection Principles for the 21st century: Revising the 1980 OESO guidelines*. Oxford: Oxford Internet Institute

Citron, D.K. & F. Pasquale (2014) The scored society: Due process for automated predictions, *Washington Law Review* 89(1).

Coeckelbergh, M. (2010). Health care, capabilities, and AI assistive technologies. In: *Ethical Theory and Moral Practice* 13(2), pp. 181-190.

College voor de Rechten van de Mens (2015) *Strategisch Plan 2016-2019*. Utrecht: College voor de Rechten van de Mens.

Compen, N., J. Ham & A. Spahn (2014) Duurzaamheidscoaches. Een beter milieu begint met jouw coach. In: L. Kool, J. Timmer & R. van Est (red.) *Eerlijk advies – De opkomst van de e-coach*. Den Haag, Rathenau Instituut, pp. 111-128.

Cuijpers, C. M. K. C., & Koops, E. J. (2012). Smart metering and privacy in Europe: Lessons from the Dutch case. In S. Gutwirth, R. E. Leenes, P. de Hert, & Y. Poulet (Eds.), *European data protection: Coming of age*. (pp. 269-293).

D66 (2016) *Concept-verkiezingsprogramma. Samen sterker – kansen voor iedereen*. Den Haag: D66.

Datta, A. & M.C. Tschantz, & A. Datta (2015) Automated experiments on ad privacy settings. A tale of opacity, choice, and discrimination. In: *Proceedings on Privacy Enhancing Technologies*, 2015(1), pp. 92–112.

De Hert, P.J.A. & A.C.J. Sprokkereef, (2012) Second generation biometrics: The ethical, legal and social context. In: E. Mordini & D. Tzovaras (red.) *Biometrics, Privacy and Agency*, Berlijn: Springer, pp. 81-101.

De Vriend, H. (2006) *Een Raad voor Ethiek en Biotechnologie: Verslag van een conferentie (Den Haag, 4 december 2006)*. Rijswijk: LisConsult.

Deloitte (2014) *De impact van automatisering op de Nederlandse arbeidsmarkt. Een gedegen verkenning op basis van Data Analytics*. Deloitte

Diakopoulos, N. (2016) Accountability in algorithmic decision making. In: *Communications of the ACM* 59(2), 56-62.

Dijk, van J. (1997) *De netwerkmaatschappij. Sociale aspecten van nieuwe media*. Houten: Bohn Stafleu Van Loghum

Dotson, T. (2014) Authentic virtual others? The promise of post-modern technologies. In: *AI & Society* 29(1), pp. 11-21.

Dratwa, J. (Ed) (2014) *Ethics of Security and Surveillance Technologies. Opinion No 28 of the European Group on Ethics in Science and New Technologies*. Brussels, 20 mei 2014.

Dwoskin, E., Rusli, E. (2015) The Technology that Unmasks Your Hidden Emotions. In: *Wall Street Journal*. 28-01-0215. Online beschikbaar: [wsj.com/articles/startups-see-your-face-unmask-your-emotions-1422472398#:bLk8dH\\_DkLSJvA](https://www.wsj.com/articles/startups-see-your-face-unmask-your-emotions-1422472398#:bLk8dH_DkLSJvA)

EC (2011) *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights*. [https://ec.europa.eu/anti-trafficking/publications/european-commission-sector-guides-implementing-un-guiding-principles-business-and-hum-0\\_en](https://ec.europa.eu/anti-trafficking/publications/european-commission-sector-guides-implementing-un-guiding-principles-business-and-hum-0_en)

EDPS (2015) *Towards a new digital ethics: Data dignity and technology, Opinion 4/2015*. Brussel: European Data Protection Supervisor.

EDPS (2016) *Press Release: EDPS starts work on a New Digital Ethics*, EDPS/2016/05. Brussels.

Eskens, S., J. Timmer, L. Kool, & R. van Est (2016) *Beyond control. Exploratory study on the discourse in Silicon Valley about consumer privacy in the Internet of Things*. Den Haag: Rathenau Instituut.



Est, R. van, D. Stemerding, V. Rerimassie, M. Schuijff, J. Timmer & F. Brom (2014) *From Bio to NBIC convergence – From Medical Practice to Daily Life*. Report written for the Council of Europe, Committee on Bioethics. Den Haag: Rathenau Instituut.

Est, R. van, & L. Kool (red.) (2015) *Werken aan de robotsamenleving. Visies en inzichten uit de wetenschap over de relatie technologie en werkgelegenheid*. Den Haag: Rathenau Instituut.

Est, R. van, & V. Rerimassie (2014) *Strijd om onze intimiteit. Het Bericht*. Den Haag: Rathenau Instituut.

Est, R. van, m.m.v. V. Rerimassie, I. van Keulen & G. Dorren (2014). *Intieme technologie. De slag om ons lichaam en gedrag*. Den Haag: Rathenau Instituut.

Est, van R., & Kool, L. (red.) (2015) *Werken aan de robotsamenleving. Visies en inzichten uit de wetenschap over de relatie technologie en werkgelegenheid*. Den Haag, Rathenau Instituut.

Est, R. van, J. Timmer, L. Kool, N. Nijsingh, V. Rerimassie & D. Stemerding, (2016) *Rules for the digital human park. Two paradigmatic cases of breeding and taming human beings: Human germline editing and persuasive technology*. Background Paper for the 11<sup>th</sup> Global Summit of National Ethics Committees, Berlin.

Van Est, R. en Gerritsen, J. (Nog te verschijnen). *Human rights in the robot age. Challenges due to the use of robotics, artificial intelligence, virtual and augmented reality*. Export report written for Council of Europe, Parliamentary Assembly, Committee on Culture, Science, Education and Media. Rathenau Instituut: Den Haag.

Van Est, R. (2016). *Technologisch burgerschap als dé democratische uitdaging van de eenentwintigste eeuw*. Christen Democratische Verkenningen. 2016(3). Amsterdam: Boom Uitgevers.

Floridi, L. (red.) (2013) *The Onlife Manifesto. Being Human in a Hyperconnected Era*. New York: Springer Publishing.

Fogg, B.J. (2002) *Persuasive Technology: Using Computers to Change What We Think and Do*. Boston: Morgan Kaufmann.

Ford, M. (2015) *The Rise of the Robots. Technology and the Threat of a Jobless Future*. New York: Basic Books.

Frenken, K., T. Meelen, M. Arets & P. van de Glind (2015). Wat is nu eigenlijk deeleconomie? In: *Me Judice*, 27 maart.

Frey, C.B. & M.A. Osborne (2013) *The Future of Unemployment. How Susceptible Are Jobs to Computerization*. Oxford: Oxford Martin Publication.

Future of Life Institute (2015) *Autonomous Weapons: An open letter from AI & Robotics researchers*, [futureoflife.org/open-letter-autonomous-weapons/](http://futureoflife.org/open-letter-autonomous-weapons/)

Gartner (2015). *Gartner Says 6.4 Billion Connected 'Things' Will Be in Use in 2016, Up 30 Percent From 2015*. Gartner Press Release. November 10, 2015. [gartner.com/newsroom/id/3165317](http://gartner.com/newsroom/id/3165317)

GCIG (Global Commission on Internet Governance) (2016) *Our Internet*. Ontario / London: Centre for International Governance Innovation / Chatham House.

Geser, H. (2010). Augmenting things, establishments and human beings. In: *Sociology in Switzerland: Towards Cybersociety and Virtual Social Relations* (Zürich, Maart 2010) ([socio.ch/intcom/t\\_hgeser24.pdf](http://socio.ch/intcom/t_hgeser24.pdf)).

Gezondheidsraad (2006) *Betekenis van nanotechnologieën voor de gezondheid*. Den Haag: Gezondheidsraad.

Gibbs, S. (2014) Elon Musk: artificial intelligence is our biggest existential threat. In: *The Guardian*. 27-10-2014.

Gibbs, S. (2015) Samsung's voice-recording smart TVs breach privacy law, campaigners claim. In: *The Guardian*, 27-02-2015. Online geraadpleegd: [theguardian.com/technology/2015/feb/27/samsung-voice-recording-smart-tv-breach-privacy-law-campaigners-claim](http://theguardian.com/technology/2015/feb/27/samsung-voice-recording-smart-tv-breach-privacy-law-campaigners-claim)

Gillespie, T. (2014). The relevance of algorithms. In: T. Gillespie, P.J. Boczkowski & K.A. Foot (eds.) *Media Technologies: Essays on Communication, Materiality, and Society*. MIT Press Scholarship Online (doi:10.7551/mitpress/9780262525374.001.0001).

Goodall, N.J. (2014). Ethical decision making during automated vehicle crashes. Transportation Research Record. In: *Journal of the Transportation Research Board* 2424, pp. 58-65.

Goodwin, T. (2015) The Battle Is for the Customer Interface. In: *TechCrunch*, 3 maart. [techcrunch.com/2015/03/03/in-the-age-of-disintermediation-thebattle](http://techcrunch.com/2015/03/03/in-the-age-of-disintermediation-thebattle)

Greenberg, A. & K. Zetter (2015). How the Internet of Things Got Hacked. In: *Wired*, 28-12-2015. Online beschikbaar: [wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked](http://wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked)

Ham, J., C. Midden & F. Beute (2009) *Unconscious Persuasion by Ambient Persuasive Technology. Evidence for the Effectivity of Subliminal Feedback*. Edinburgh: Proceedings of Artificial Intelligence and Simulation of Behaviour Conference.

Harris, D. (2015) Google: Our new system for recognizing faces is the best one ever. In: *Forbes*, 17-03-2015.

Hawking, S., S. Russell, M. Tegmark & F. Wilczek (2014) Stephen Hawking: Transcendence looks at the implications of artificial intelligence - but are we taking AI seriously enough? In: *The Independent*. 01-05-2014.

Heimo, O.I., A. Hakkala & K.K. Kimppa (2012). How to abuse biometric passport systems. In: *Journal of Information. Communication and Ethics in Society* 10(2), pp. 68-81.

Helbing et al. (2015) Digitale Democratie statt Datendiktatur. Digital Manifest. In: *Spektrum der Wissenschaft*, pp. 50-61.

Hern, A. (2014) Hacker fakes German minister's fingerprints using photos of her hands, *The Guardian*, 30-12-2014. Online beschikbaar: [theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands](http://theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands)

Hessels, L. en Van Deuten, J. (2012). *Coördinatie van publiek-privaat onderzoek. Van variëteit naar maatwerk*. Rathenau Instituut: Den Haag

Hildebrandt, M. (2012). The dawn of a critical transparency right for the profiling era. In: J. Bus (red.), *Digital Enlightenment Yearbook 2012*. Amsterdam: IOS Press. pp. 41-56.

Hildebrandt, M. (2015). *Smart technologies and the end(s) of law: Novel entanglements of law and technology*. Cheltenham, UK: Edward Elgar publishing.

Hildebrandt, M. (2016) Data gestuurde intelligentie in het strafrecht'. In E.M.L. Moerel, J.E.J. Prins, M. Hildebrandt, T.F.E Tjong Tjin Tai, G-J. Zwenne en A.H.J. Schmidt, Homo Digitalis. In: *Handelingen Nederlandse Juristen-Vereniging 146e jaargang/2016-I*, pp. 137-240, Wolters Kluwer, Beschikbaar op: [njv.nl/wp-content/uploads/2011/04/Preadviezen-NJV-2016.pdf](http://njv.nl/wp-content/uploads/2011/04/Preadviezen-NJV-2016.pdf)

Hill, K. (2015) This guy's light bulb performed a DoS attack on his entire smart house. In: *Fusion*, 03-03-2015. Online beschikbaar: [fusion.net/story/55026/this-guys-light-bulb-ddosed-his-entire-smart-house/](http://fusion.net/story/55026/this-guys-light-bulb-ddosed-his-entire-smart-house/)

Hilty, L.M. (2015) Ethical issues in ubiquitous computing – Three technology assessment studies revisited. In: K. Kinder-Kurlanda & C. Ehrwein Nihan (red.), *Ubiquitous Computing in the Workplace*. Dordrecht, Springer.

Hof, C van 't., C. Daemen, R. van Est (red.) (2010) *Check-in, check-out. De digitalisering van de openbare ruimte*. Den Haag: Rathenau Instituut.

Hof, C. van 't, J. Timmer & R. van Est (red.) (2012a) *Voorgeprogrammeerd: hoe internet ons leven leidt*. Boom Lemma.

Hof, C. van 't, J. Timmer & R. van Est (2012b) *Het Bericht: Voorgeprogrammeerd – Online keuzevrijheid onder druk*. Den Haag: Rathenau Instituut.

IBM (2013). *IBM Research Unveils Two New Watson Related Projects from Cleveland Clinic Collaboration*. [ibm.com/press/us/en/pressrelease/42203.wss](http://ibm.com/press/us/en/pressrelease/42203.wss)

IDC (2011) *Extracting Value from Chaos*, IDC Digital Universe study. Online beschikbaar: [emc.com/about/news/press/2011/20110628-01.htm](http://emc.com/about/news/press/2011/20110628-01.htm)

IDC (2014) *Digital Universe of opportunities: Rich data and the increasing value of the Internet of Things*. IDC Digital Universe study.

IEEE (2016) *The Global Initiative for Ethical Consideration in the Design of Autonomous Systems*. IEEE. Online beschikbaar: [standards.ieee.org/develop/indconn/ec/ec\\_about\\_us.pdf](http://standards.ieee.org/develop/indconn/ec/ec_about_us.pdf)  
[is-all-for-the-customer-interface/](http://standards.ieee.org/develop/indconn/ec/ec_about_us.pdf)

Ismail, I., M.S. Malone & Y. van Geest (2014) *Exponential Organizations. Why New Organizations Are Ten Times Better, Faster, and Cheaper than Yours (and What To Do About It)*. New York: Diversionbooks.

ITU (2005) *The Internet of Things*. [itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf](http://itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf)

Janssen, A., L. Kool, en J. Timmer (2015) *Dicht op de huid. Gezichts- en emotieherkenning in Nederland*. Den Haag: Rathenau Instituut.

Juul, N.C. (2015) Recommendation on the use of biometric technology. In: P. Campisi (red). *Security and Privacy in Biometrics*. Londen, Springer Verlag, pp. 415-433.

Kaptein, M. & D. Eckles (2012) Heterogeneity in the Effects of Online Persuasion. In: *Journal of Interactive Marketing* 25, pp. 176-188.

Kaptein, M., Markopoulos, P., Ruyter, B. de, Aarts, E. (2015) Personalizing persuasive technologies: Explicit and implicit personalization using persuasion profiles. In: *International Journal of Human-Computer Studies* 77, pp. 38-51. doi:10.1016/j.ijhcs.2015.01.004

Karppinen, P. & H. Oinas-Kukkonen (2013) Three approaches to ethical considerations in the design of behavior change support systems. In: *PERSUASIVE'13 Proceedings of the 8th international conference on Persuasive Technology*, Heidelberg, Springer-Verlag, pp. 87-98.

KEMO (2004) *Kerncommissie Ethiek Medisch Onderzoek (KEMO) 1993-1999*. Den Haag: KEMO.

Kiss, J. (2014) An online Magna Carta: Berners-Lee calls for bill of rights for web. In: *The Guardian*, 12-03-2014. Online beschikbaar: [theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web](http://theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web)

Kizza, J.M. (2013) *Ethical and Social Issues in the Information Age*. Heidelberg, Springer.

KLPD – Dienst Nationale Recherche (2008) *Schone schijn: De signalering van mensenhandel in de vergunde prostitutiesector*. Driebergen: KLPD.

Knight, W. (2015) Inside Amazon's Warehouse, Human-Robot Symbiosis. In: *Technology Review*. 07-07-2015. Online beschikbaar: [technologyreview.com/news/538601/inside-amazons-warehouse-human-robot-symbiosis](http://technologyreview.com/news/538601/inside-amazons-warehouse-human-robot-symbiosis)

Kollanyi, B., P.N. Howard & S.C. Woolley (2016) Bots and Automation over Twitter during the First U.S. Presidential Debate. In: *Computational Propaganda Data Memo* 2016.1, 14-10-2016

Kool, L., J. Timmer & R. van Est (2014) *Eerlijk advies. De opkomst van de e-coach*. Den Haag: Rathenau Instituut.

Kool, L., J. Timmer & R. van Est (2015) *De datagedreven samenleving. Achtergrondstudie*. Den Haag, Rathenau Instituut.

Koops, E. J. (2011) Digitale grondrechten en de staatscommissie: Op zoek naar de kern. In: *Tijdschrift voor constitutioneel recht* 2(2), pp. 168-185.

Koops, E. J. & Prinsen, M. M. (2005) Glazen woning, transparant lichaam: een toekomstblik op huisrecht en lichamelijke integriteit. In: *Nederlands Juristenblad* 80(12), pp. 624-630.

Koops, E.J. (2014) Privacy, informatieveiligheid en een onzichtbare medaille. In: S. Kok et al. (red.) *Informatieveiligheid*. Taskforce Bestuur & Informatieveiligheid Dienstverlening, pp. 57-73.

Kosinski, M., D. Stillwell & T. Graepel (2013) Private traits and attributes are predictable from digital records of human behavior. In: *PNAS* 110(15), pp. 5802–5805.

Kramer, A.D.I, J.E. Guillory & J.T. Hancock (2014). Experimental evidence of massive-scale emotional contagion through social networks. In: *PNAS* 111(24), pp. 8788-8790.

Kreijveld, M. (2014) De kracht van platformen. Nieuwe strategieën voor innoveren in een digitaliserende wereld. Den Haag, Rathenau Instituut.

Kreijveld, M., J. Deuten & R. van Est (red.) (2014) *De kracht van platformen. Nieuwe strategieën voor innoveren in een digitaliserende wereld*. Den Haag/Deventer: Rathenau Instituut/Vakmedianet.

Ladikas, M., S. Chaturvedi, Y. Zhao & D. Stemerding (red.) (2015) *Science and technology governance and ethics: A global perspective from Europe, India and China*, Heidelberg: Springer

Li, X., X. Hong, A. Moilanen, X. Huang, T. Pfister, G. Zhao & M. Pietikäinen (2015) *Reading Hidden Emotions: Spontaneous Micro-expression Spotting and Recognition*. arXiv:1511.00423 [cs.CV]

Louv, R. (2005) *Last child in the woods: Saving our children from nature-deficit disorder*. Chapel Hill, NC: Algonquin Books.

Maan, S., B. Merkus, J. Ham & C. Midden (2011). Making it not too obvious. The effect of ambient light feedback on space heating energy consumption. In: *Energy Efficiency* 4(2), pp. 175-183.

Madary, M. & T.K. Metzinger (2016) Real virtuality: A code of ethical conduct. Recommendations for good scientific practice and the consumers of VR-technology. In: *Frontiers in Robotics and AI* 3 (19 februari).

Martijn, M. (2016) Deze professor probeert privacy opnieuw uit te vinden en dat is broodnodig. In: *De Correspondent*, 8 augustus. Online beschikbaar: [decorrespondent.nl/5043/Deze-professor-probeert-privacy-opnieuw-uit-te-vinden-en-dat-is-broodnodig/155102508-199b13c9](http://decorrespondent.nl/5043/Deze-professor-probeert-privacy-opnieuw-uit-te-vinden-en-dat-is-broodnodig/155102508-199b13c9)

Mayer-Schonberger, V. & K. Cukier (2013) *Big Data: A Revolution that Will Transform How we Live, Work and Think*. Houghton: Mifflin Harcourt.

Meelen, T. & K. Frenken (2014) UberPop is geen voorbeeld van deeleconomie. In: *Het Parool*, 10 oktober.

Melson, G.F., P.H. Kahn, A. Beck & B. Friedman (2009) Robotic pets in human lives: Implications for the human-animal bond and for human relationships with personified technologies. In: *Journal of Social Issues* 65(3), pp. 545-569.

Meulen, van der, B. & A. Rip (1998) Mediation in the Dutch science system. In: *Research Policy* 27(8) pp. 757-769.

Michael, K. & M.G. Michael (2013) The future prospects of embedded microchips in humans as unique identifiers: the risks versus the rewards. In: *Media Culture and Society* 35(1), pp. 78-86.

Ministerie van Binnenlandse Zaken (2013) *Visiebrief digitale overheid 2017*, [rijksoverheid.nl/documenten/kamerstukken/2013/05/23/visiebrief-digitale-overheid-2017](http://rijksoverheid.nl/documenten/kamerstukken/2013/05/23/visiebrief-digitale-overheid-2017)

Misa, T.J., P. Brey & A. Feenberg (red.) (2003) *Modernity and Technology*. Cambridge, MA: The MIT Press.

Moerel, L. (2015) Zo behouden alleen de rijken hun privacy. In: *NRC Handelsblad*, 28 november. Online beschikbaar: [nrc.nl/nieuws/2015/11/28/zo-behouden-alleen-de-rijken-hun-privacy-1561104-a579887](http://nrc.nl/nieuws/2015/11/28/zo-behouden-alleen-de-rijken-hun-privacy-1561104-a579887)

Morozov, E. (2013) *To Save Everything, Click Here: The Folly of Technological Solutionism*. Londen, PublicAffairs.

Mul, de, J. (1999) The Informatization of the Worldview. In: *Information, Communication & Society* 2(1), pp. 604-629.

Nanopodium (2011) *Verantwoord verder met nanotechnologie. Bevindingen maart 2009 – januari 2011*. Eindrapport Commissie Maatschappelijke Dialoog Nanotechnologie.

Negroponte, N. (1995) *Being Digital*. New York: Alfred A. Knopf.

NL next level (2016) *Investeren in een digitale kwantumsprong*. Uitgave van VNO-NCW, MKB-Nederland, LTO-Nederland, september 2016. Online beschikbaar: [nl-nextlevel.nl/wp-content/uploads/2016/09/de\\_digitale\\_kwantumsprong.pdf](http://nl-nextlevel.nl/wp-content/uploads/2016/09/de_digitale_kwantumsprong.pdf)

Nouwt, J., P.H. Blok, B.J. Koops, M.H.M. Schellekens, E. Schreuders & M. de Vries (2000) Grondrechten in het digitale tijdperk. In: *Nederlands Juristenblad* 75(27), pp. 1321-1327.

NSOB & PBL (2014) *Leren door doen. Overheidsparticipatie in een energieke samenleving*. Den Haag. Den Haag: NSOB & PBL

O'Brolchain, F., T. Jacquemard, D. Monaghan, N. O'Connor, P. Novitzky & B. Gordijn (2016) The convergence of virtual reality and social networks: Threats to privacy and autonomy. In: *Science and Engineering Ethics* 22(1), pp. 1-29.

O'Reilly, T. (2005) *What Is Web 2.0. Design Patterns and Business Models for the Next Generation of Software*. 30/9/2005 [oreilly.com/pub/a/web2/archive/what-is-web-20.html](http://oreilly.com/pub/a/web2/archive/what-is-web-20.html)

OESO (2013), *Building Blocks for Smart Networks*, OECD Digital Economy Papers, No. 215, OECD Publishing. [oecd-ilibrary.org/science-and-technology/building-blocks-for-smart-networks\\_5k4dkhvnzv35-en](http://oecd-ilibrary.org/science-and-technology/building-blocks-for-smart-networks_5k4dkhvnzv35-en)

Owen, R. P. Macnaghten & J. Stilgoe (2012) Responsible research and innovation: From science in society to science for society, with society. In: *Science and Public Policy* 39(6), pp. 751-760.

Pariser, E. (2011) *The filter bubble: What the Internet is hiding from you*. New York, Penguin Press.

Pasquale, F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge MA: Harvard University Press.

Peck, D. (2013) They're watching you at work. In: *The Atlantic*, december 2013. Online beschikbaar: [theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681](http://theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681)

Peppet, S.R. (2014) Regulating the Internet of Things: First steps towards managing discrimination, Privacy, Security and Consent, 93. In: *Texas Law Review* 93, pp. 85-176.

Pereira, A.G., A. Benessia & P. Curvelo (2013) *Agency in the Internet of Things*. Luxembourg: Publications Office of the European Union.

Podesta, J., P. Pritzker, E. Moniz, J. Holdren & J. Zients (2014) *Big Data: Seizing opportunities, preserving values*. Washington: Executive Office of the President.

Poel, M. (2010) *Verbreiding en vervlechting van het Nederlandse ICT-beleid. Rationale, beleidsinstrumenten en beleidscoördinatie*. Essay op uitnodiging van het Ministerie van Economische Zaken, Directoraat Generaal Energie en Telecom.

PWC (2013) *Omvang van identiteitsfraude & maatschappelijke schade in Nederland*. PricewaterhouseCoopers.

Radboud Universiteit (2016) *Bart Jacobs zet digitale beveiliging op de kaart*. Online beschikbaar: [ru.nl/onderzoek/over/vm/onderzoeksthema/informatica-digitale/vm/professor-bart](http://ru.nl/onderzoek/over/vm/onderzoeksthema/informatica-digitale/vm/professor-bart)

Ramthun, S. & C. Schlesiger (2016) Dobrindt gründet Ethikkommission für automatisiertes Fahren. In: *Wirtschafts Woche*. Online beschikbaar: [wiwo.de/politik/europa/selbstfahrende-autos-dobrindt-gruendet-ethikkommission-fuer-automatisiertes-fahren/14513384.html](http://wiwo.de/politik/europa/selbstfahrende-autos-dobrindt-gruendet-ethikkommission-fuer-automatisiertes-fahren/14513384.html)

Rani, A. (2013) The Japanese men who prefer virtual girlfriends to sex. In: *BBC*, 24-10-2013. Online beschikbaar: [bbc.com/news/magazine-24614830](http://bbc.com/news/magazine-24614830)

Renaud, K., A. Hoskins & R. von Solms (2015) Biometric identification: Are we ethically ready? In: *Information Security for South Africa (ISSA)*. Johannesburg, August, pp. 12-13.

Rerimassie, V. & F. Brom (2012) Science and technology ethics structure in the Netherlands. In: *Global Ethics in Science and Technology Deliverable D1.1 Ethics state of the art EU Debate*, p. 55-61.

Rli (2015) *Werkprogramma 2015-2016*. Den Haag: Raad voor de leefomgeving en infrastructuur.

Rli (2015a) *Verkenning technologische innovaties in de leefomgeving. Januari 2015*. Den Haag: Raad voor de leefomgeving en infrastructuur.

Rogers, B. (2015) The Social Costs of Uber. In: *The University of Chicago Law Review Dialogue* 82(85), pp. 85-102.

Roman, R., J. Zhou, & J. Lopez (2013) On the features and challenges of security and privacy in distributed Internet of Things. In: *Computer Networks* 57(10), pp. 2266-2279.

Royackers, L. en R. van Est (2015) *Just ordinary robots. Automation from love to war*. Boca Raton, FL: CRC Press.

RVS (2016) *Over de RVS*. Online beschikbaar: [raadrvs.nl/raad/over-rvs](http://raadrvs.nl/raad/over-rvs)

Von Schomberg, R. (2011) Prospects for Technology Assessment in a framework of responsible research and innovation. In: M. Dusseldorp & R. Beecroft (red.) *Technikfolgen abschätzen lehren: Bildungspotenziale transdisziplinärer Methode*. Wiesbaden: Springer, pp. 39-61.

Scholz, L.H. (2016a) Algorithmic contracts. In: *Stanford Technology Law Review* (forthcoming).

Scholz, T. (2016b) *Platform cooperativism. Challenging the corporate sharing economy*. New York: Rosa Luxemburg Stiftung.



Seddon, R.F.J. (2013) Getting 'virtual' wrongs right. In: *Ethics and Information Technology* 15(1), pp. 1-11.

Sharkey, A. (2014) Robots and human dignity: A consideration of the effects of robot care on the dignity of older people. In: *Ethics and Information Technology* 16(1), pp. 63-75.

Sharkey, N. (2010) Saying 'no!' to lethal autonomous targeting. In: *Journal of Military Ethics* 9(4), pp. 369-383.

Shead, S. (2016) The biggest mystery in AI right now is the ethics board that Google set up after buying DeepMind. In: *Business Insider*, 26 maart 2016. Online beschikbaar: [uk.businessinsider.com/google-ai-ethics-board-remains-a-mystery-2016-3](http://uk.businessinsider.com/google-ai-ethics-board-remains-a-mystery-2016-3)

Sloot, van der, B. (2014). De noodzaak om privacy als publiek belang te herformuleren. In: *Christen Democratische Verkenningen* 3, pp. 125-132. Amsterdam: Boom Uitgevers

Smids, J. (2012) The voluntariness of persuasive technology. In: M. Bang & E.L. Ragnemalm (red.) *PERSUASIVE 2012. LNCS 7284*, Springer, Heidelberg, pp. 123–132.

Solove, D.J. (2002) Conceptualizing Privacy. In: *California Law Review* 2002(4), pp. 1087-1156.

Spahn, A. (2011) And lead us (not) into persuasion...? Persuasive technology and the ethics of communication. In: *Science and Engineering Ethics* 18(4), pp. 1-18.

Spahn, A. (2013) Ideas in motion. Moralizing mobility? Persuasive technologies and the ethics of mobility. In: *Transfer* 3(2), pp. 108-115.

Steiner, C. (2012) *Automate This: How Algorithms Came to Rule Our World*. London: Penguin Books.

Steltman, M. (2016). Aftappen ICT maakt Nederland niet veiliger. In: *Financieel Dagblad* (16 januari 2016).

Stemerding, D. & L. Kater (2005) *Public bio-ethics bodies as intermediary organisations*. Paper presented at the workshop on Intermediary Organisations, PRIME, University of Twente, 6-7 October.

Stone, B. (2009) Amazon Erases Orwell Books From Kindle. In: *New York Times*, 17-07-2009. Online beschikbaar: [nytimes.com/2009/07/18/technology/companies/18amazon.html?\\_r=1](http://nytimes.com/2009/07/18/technology/companies/18amazon.html?_r=1)

Strawser, B.J. (red.) (2013) *Killing by remote control: The ethics of an unmanned military*. Oxford: Oxford University Press.

Subirana, B., S. Sarma & E. Fleisch (2006) High resolution management. Improving Management Vision. In: *IESE Alumni Magazine*, juli-september, pp. 8-13. [iese.com/102/ingles/pdf/subirana.pdf](http://www.iese.com/102/ingles/pdf/subirana.pdf).

Sullins, J.P. (2012) Robots, love and sex: The ethics of building love machines. In: *Affective Computing* 3(4), pp. 398-409.

Sutrop (2010) Ethical issues in governing biometric technologies. In: A. Kumar & D. Zhang (red.). *Ethics and Policy of Biometrics* (Vol. 6005 of the series Lecture Notes in Computer Science). Heidelberg: Springer, pp. 102-114.

Sutrop, M. & K. Laas-Mikko (2012) From identity verification to behavior prediction: Ethical implications of second generation biometrics. In: *Review of Policy Research* 29(1), pp. 21-36.

Swart, J., J. Wolters & H. Zwart (red.) (2004) *DECs in discussie: De beoordeling van dierproeven in Nederland*. Budel: DAMON.

The Economist (2015) Artificial intelligence. The rise of machines. In: *The Economist*, 9 mei 2015.

Timmer, J. L. Kool, L. & R. van Est, (2015) Ethical issues in emerging applications of persuasive technologies. In: T. MacTavish & S. Basapur (red.) *Persuasive Technology. 10th International Conference, PERSUASIVE 2015*, Chicago, IL, USA, June 3-5, 2015, Proceedings, pp. 196-201.

Turkle, S. (2011) *Alone together: Why we expect more from technology and less from each other*. New York: Basic Books.

Turkle, S. (2015) *Reclaiming conversation. The power of talk in a digital age*. New York: Penguin Press.

UNESCO (2005) *Explanatory memorandum of Preliminary Draft Declaration on Universal Norms on Bioethics*. Paris: UNESCO.

US Department of Transport (2016) *Federal Automated Vehicles Policy. Accelerating the Next Revolution in Roadway Safety*. September 2016. Online beschikbaar: [transportation.gov/AV/federal-automated-vehicles-policy-september-2016](http://transportation.gov/AV/federal-automated-vehicles-policy-september-2016)

Veldhuis, R.N.J. (2014) *Biometrie – Op de grens tussen techniek en mens*. Oratie, 17 april, Enschede: Universiteit Twente.

Verhey, L.F.M. (2011) Grondrechten in het digitale tijdperk: driemaal is scheepsrecht? In: *Tijdschrift voor constitutioneel recht*, maart 2011, pp. 152,167.

Verbeek, P.P. (2016) Mag de baas je stiekem naar de sportschool loodsen? In: *Tubantia*, 7 juni 2016.

VNO-NCW (2016) Manifest: Samen naar een duurzame digitale samenleving. VNO-NCW. Online beschikbaar: [vno-ncw.nl/sites/default/files/ManifestSamennaareenduurzamedigitalesamenleving.pdf](http://vno-ncw.nl/sites/default/files/ManifestSamennaareenduurzamedigitalesamenleving.pdf)

Vrijenhoek, T. & M. Radstake (2016) Genen meten nieuwe stijl. Op weg naar genetische zorg van de toekomst. In: I. Geesink (red.) *De meetbare mens. Digitaal meten van het zieke en gezonde lichaam*. Den Haag: Rathenau Instituut.

Walker, S. (2016) Face recognition app taking Russia by storm may bring end to public anonymity. In: *The Guardian*, 17-05-2016. Online beschikbaar: [theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte](http://theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte)

Walsh, K. (2016) Nest Reminds Customers That Ownership Isn't What It Used to Be. In: *EFF*, 05-04-2016. Online beschikbaar: [eff.org/deeplinks/2016/04/nest-reminds-customers-ownership-isnt-what-it-used-be](http://eff.org/deeplinks/2016/04/nest-reminds-customers-ownership-isnt-what-it-used-be)

Weber, R. (2011) Accountability in the Internet of Things. In: *Computer Law & Security Review* 27(2), pp. 133–138.

Went, R., M. Kremer, A. Knottnerus (red.) (2015) *De robot de baas. De toekomst van werk in het tweede machinetijdperk*. WRR. Den Haag/Amsterdam: Amsterdam University Press.

Werson, H. (2012) *De fatale fuik: Achter de schermen van mensenhandel en gedwongen prostitutie in Nederland*. Amsterdam: Uitgeverij Carrera.

Wolf, M.J., F. Grodzinsky & K. Miller (2015) Augmented reality all around us: Power and perception at a crossroads. In: *SIGCAS Computers & Society*, 45(3), pp. 126-131.

Wright, A. & P. de Filippi (2015) *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*. Online beschikbaar: [ssrn.com/abstract=2580664](http://ssrn.com/abstract=2580664)

WRR (2016) *Big data in een vrije en veilige samenleving*. Rapport 95. Amsterdam: Amsterdam University Press.

Zarkasy (2013) *Transparent Predictions*. SSRN, [papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2324240](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2324240)

Zoeteman, C. & I. Widdershoven-Heerding (2007) Bio-ethiek: uniformiteit of maatwerk? In: *COGEM Jaarverslag 2006*, pp. 30-33.

Zureik, E. & L. Harling Stalker (2010) The cross-cultural study of privacy. In: Zureik, E. et al. (red.) *Surveillance, privacy and the globalization of personal information*. Montreal/London/Ithaca: McGillQueen University Press.

# Appendix A: Uitgebreide analyse governance-ecosysteem

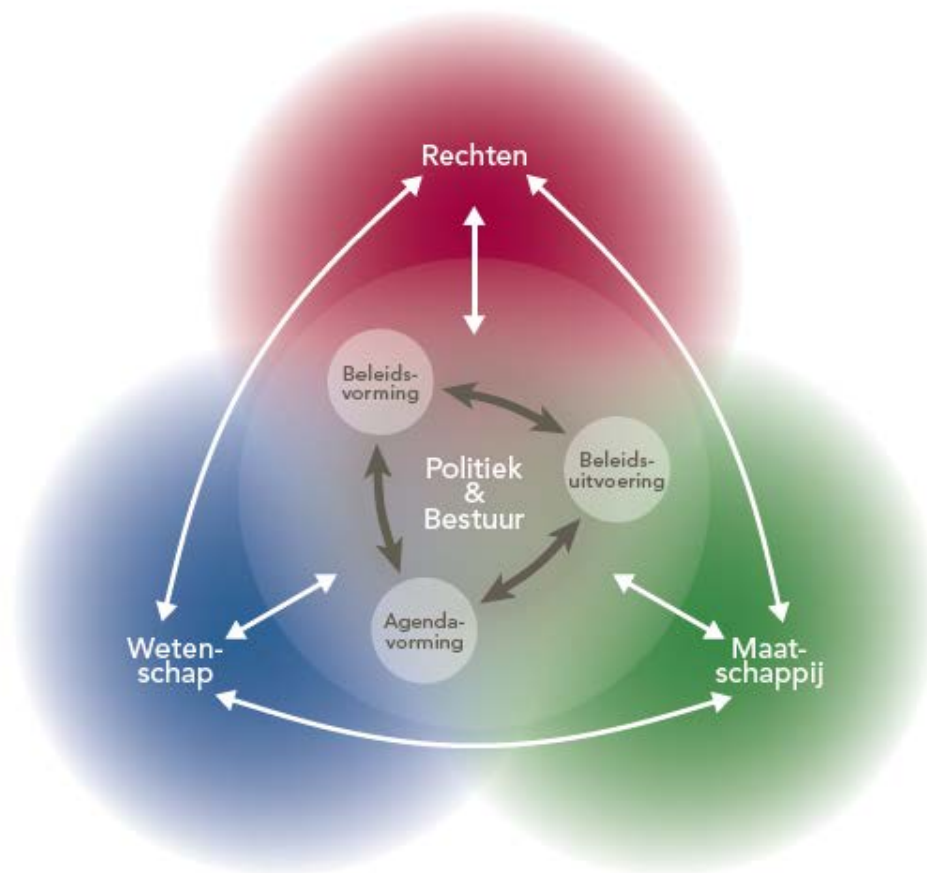
## Inleiding

In deze appendix beschrijven we de wijze waarop (de discussie over) de governance van ethische en maatschappelijke kwesties rond digitalisering de afgelopen vijf tot tien jaar vorm heeft gekregen. Dat doen we aan de hand van het conceptueel kader dat we in hoofdstuk vier hebben ontwikkeld (zie figuur 1). We beschrijven allereerst de drie domeinen van rechten, wetenschap en maatschappij. Vervolgens zoomen we in op het politiek-bestuurlijke domein. Daarbinnen beschrijven we de processen van agendavorming, beleidsvorming en beleidsuitvoering. Dit hoofdstuk is daarom als volgt opgebouwd:

- Grond- en mensenrechten (paragraaf 1.2)
- Wetenschap (paragraaf 1.3)
- Maatschappij (paragraaf 1.4)
- Politiek en bestuur
  - a. Agendavorming (paragraaf 1.5)
  - b. Beleidsvorming en –bepaling (paragraaf 1.6)
  - c. Beleidsuitvoering (paragraaf 1.7)

In iedere paragraaf gaan we op zoek naar actoren of organisaties die een institutionele rol vervullen in het betreffende domein. Onze analyse richt zich met name op ontwikkelingen in Nederland, maar benoemt ook enkele interessante buitenlandse ontwikkelingen. Op het gebied van de grond- en mensenrechten kijken we bijvoorbeeld naar de staatscommissie Thomassen, maar ook naar activiteiten van de VN Mensenrechtenraad en de Raad van Europa. Ook het domein ‘Politiek en bestuur’ beschrijven we aan de hand van de institutionele positie die een organisatie inneemt in de beleidscyclus. De acties van ministeries worden bijvoorbeeld in paragraaf 1.6 ‘Beleidsvorming’ besproken en die van de Autoriteit Persoonsgegevens in paragraaf 1.7 over ‘Beleidsuitvoering’. Dat neemt natuurlijk niet weg dat ministeries en de Autoriteit Persoonsgegevens als respectievelijk beleidsbepalende en beleidsuitvoerende organisaties, ook beleidsvoorbereidende acties kunnen ondernemen.

In deze appendix benoemen we alleen initiatieven die zich met maatschappelijke en ethische vragen rond digitalisering bezighouden. Naast een korte beschrijving van de betreffende organisatie, geven we aan met welke technologie de organisatie zich heeft beziggehouden. Acties kunnen zich bijvoorbeeld richten op een specifieke technologie, zoals drones of zelfrijdende auto's, maar ook over robotica in het algemeen, of zelfs digitalisering in het algemeen. Vervolgens bezien we voor welke ethische en maatschappelijke aspecten van digitalisering de betreffende organisatie aandacht heeft. Daarbij kijken we in hoeverre de in hoofdstuk 3 gesignaleerde kwesties al dan niet worden opgepakt. En ten slotte beschrijven we welke governance-acties diverse organisaties voorstellen, voorbereiden, initiëren of uitvoeren om in te spelen op maatschappelijke en ethische kwesties die verband houden met de digitalisering van de samenleving.

**Figuur 1** Raamwerk voor het governance-ecosysteem

Rathenau Instituut

## Grond- en mensenrechten

Grond- en mensenrechten vormen de basis waarin maatschappelijke waarden en fundamentele vrijheden zijn vastgelegd. Deze rechten zijn vastgelegd in door Nederland geratificeerde internationale verdragen, zoals de Universele Verklaring van de Rechten van de Mens van de Verenigde Naties (1948), of in de Nederlandse Grondwet. Ze verankeren voor Nederland belangrijke waarden zoals menselijke waardigheid, vrijheid, veiligheid, gelijkheid en rechtvaardigheid. In hoofdstuk 3 zagen we dat digitalisering kan raken aan vele fundamentele menselijke waarden en rechten. In deze paragraaf beschrijven we de discussie in Nederland over de vraag of, en zo ja, op welke wijze onze Grondwet aangepast dient te worden aan het digitale tijdperk. Daarnaast laten we zien dat een dergelijke discussie ook buiten onze landsgrenzen gevoerd wordt. We benoemen enkele activiteiten die binnen de Raad van Europa en de Mensenrechtenraad van de Verenigde Naties zijn gedaan op het gebied van mensenrechten en digitalisering.

### Digitalisering en de Nederlandse Grondwet<sup>94</sup>

Kabinet Balkenende IV stelde op 9 juli 2009 de staatscommissie Thomassen in om te adviseren over een mogelijke herziening van de grondwet. Daarbij werd ook de vraag naar de invulling van grondrechten in het digitale tijdperk meegenomen. De commissie Thomassen adviseerde in 2010 in haar eindrapport om de Grondwet op enkele punten te actualiseren. De voorgestelde wijzigingen beoogen op een technologie-neutrale manier invulling te geven aan artikel 7 (vrijheid van meningsuiting), artikel 10 (eerbiediging persoonlijke levenssfeer) en artikel 13 (vertrouwelijke communicatie). Het kabinet besloot om alleen artikel 13 te wijzigen (Kamerstukken II 2010-2011, 31570, nr. 20). Deze grondwetswijziging is op dit moment nog in behandeling.<sup>95</sup> Het advies van de commissie Thomassen en de voorgestelde grondwetswijziging brachten ook een bredere discussie met zich mee over grondrechten in het digitale tijdperk. Verschillende auteurs bepleiten dat digitalisering vraagt om een brede bezinning over de vraag hoe in constitutionele zin met technologische verandering moet worden omgegaan (Koops 2011; Prins 2015).

Behalve discussie over wat de Nederlandse Grondwet zou moeten beschermen in het digitale tijdperk is er ook discussie over hoe die bescherming kan worden ingeroepen. Om de normatieve werking van de Grondwet te versterken, adviseerde de commissie Thomassen het toetsingsverbod op de Grondwet (artikel 120 van de Grondwet) te laten vervallen. Dit advies werd niet overgenomen, maar blijft een punt van discussie (Dommering 2011; Raad voor de Rechtspraak 2014; Kamerstukken II 2013-2014, 32334, nr. 8). Toetsing aan de Grondwet zou individuele burgers, NGO's en burgerrechtenorganisaties namelijk meer mogelijkheden kunnen bieden om hun recht te halen als het gaat om door de Grondwet beschermde rechten, zoals de eerbiediging van de persoonlijke levenssfeer. NGO Privacy First geeft aan dat toetsing aan de Grondwet voor hen een belangrijk middel zou kunnen zijn dat bijdraagt aan de bescherming van privacy als mensenrecht.<sup>96</sup> Om een beroep te doen op het recht op eerbiediging van de persoonlijke levenssfeer wordt nu veelal uitgeweken naar het Europese Verdrag van de Rechten van de Mens (EVRM). In de discussie over toetsing aan de Grondwet zijn er ook tegenstanders die pleiten dat de toetsing aan internationale verdragen moet worden afgeschaft (Kamerstukken II, 2013-2014, 33 359, nr.5). Naast de rechter speelt ook het College voor de Rechten van de Mens een rol in het toezien op de mensenrechten. Het College doet dat door onderzoek, advies, voorlichting en het individueel oordelen in het geval van discriminatie. Waar digitalisering de mensenrechten raakt zou het College een rol kunnen spelen. Het onderwerp van digitalisering staat echter niet expliciet op de agenda van het College (College voor de Rechten van de Mens 2016).

---

<sup>94</sup> In hoofdstuk 4 beschreven we reeds dat de discussie over actualisering van de Nederlandse Grondwet reeds in de tweede helft van de jaren negentig startte met de instelling van de staatscommissie Franken (1999-2000). De voorstellen tot grondwetswijzigingen die op basis van het advies van deze commissie werden opgesteld werden niet overgenomen na kritiek van de Raad van State in 2004 (Verhey 2011; Koops 2011). Zie Kamerstukken II 2000-2001, 27460, nr. 1 en het rapport 'Commissie grondrechten in het digitale tijdperk' (2000) van de commissie Franken.

<sup>95</sup> Zie voor de huidige status [denederlandsegrondwet.nl/9353000/1/j9vviHf299q0sr/vjInm176ini](http://denederlandsegrondwet.nl/9353000/1/j9vviHf299q0sr/vjInm176ini)

<sup>96</sup> Gesprek Stichting Privacy First 24-05-2016

## Internationale ontwikkelingen

### *Verenigde Naties: Bescherming mensenrechten in de digitale wereld*

Met name de VN Mensenrechtenraad (*Human Rights Council, HRC*) houdt zich bezig met de relatie tussen digitalisering en mensenrechten. In 2011 bepleitte La Rue – tussen 2008 en 2014 Speciale Rapporteur van de VN Mensenrechtterraad aangaande de promotie en bescherming van het recht op vrijheid van mening en meningsuiting – wettelijke garanties voor universele internettoegang. Landen zoals Duitsland, Finland en Estland hebben voorzichtige stappen in deze richting gezet (Prins 2015). Op 6 juli 2012 stemde de Mensenrechtenraad unaniem in met Resolutie L13 *The promotion, protection and enjoyment of human rights on the Internet*. Deze zogenoemde Internet Resolutie<sup>97</sup> stelt dat de rechten die mensen in de fysieke wereld (*offline*) hebben ook in de digitale wereld (*online*) beschermd dienen te worden. Daarmee wordt de Universele Verklaring van de Rechten van de Mens van de Verenigde Naties uit 1948, alsmede andere relevante internationale mensenrechtenverdragen, heel duidelijke herbevestigd voor het digitale tijdperk. In 2015 stelde de VN Mensenrechtenraad (Human Rights Council) Joe Cannataci aan als eerste Speciale Rapporteur op het gebied van het recht op privacy met als taak het verzamelen van informatie en het opstellen van aanbevelingen ter promotie van het recht op privacy (resolutie 28/16). Verder uitte de Algemene Vergadering in 2013 haar zorgen over de negatieve impacts van surveillance op mensenrechten (resolutie 68/167). Binnen de UNESCO bereiden het IBC (International Bioethics Committee) en COMEST (World Commission on the Ethics of Scientific Knowledge and Technology) rapporten voor op het gebied van, respectievelijk, big data & health en robotica, die in het najaar van 2017 zullen verschijnen.

### *Raad van Europa: Verbreding ethisch werkveld vanwege technologische convergentie*<sup>98</sup>

Ook binnen de Raad van Europa<sup>99</sup> groeit de aandacht voor de invloed van digitalisering. Begin jaren tachtig was de Raad van Europa een van de eerste instituties die de bescherming van privacy op de internationale agenda plaatste en diverse centrale principes omschreef voor de eerlijke omgang met en bescherming van persoonlijke gegevens (Bennet & Raab 2006). Vanaf de jaren negentig speelt de Raad van Europa een belangrijke rol op het raakvlak van de gebied van de ethiek, biotechnologie en geneeskunde. In 1991 beval de Parlementaire Vergadering van de Raad van Europa (PACE) aan een Verdrag inzake bio-ethiek voor te bereiden. Dit leidde in 1997 tot het Verdrag inzake de rechten van de mens en de biogeneeskunde, het zogenoemde Verdrag van Oviedo.

Sinds 2013 is de Committee on Bioethics (DH-BIO) van de Raad van Europa bezig met de talloze implicaties die het samenkomen van diverse technologische ontwikkelingen – waaronder

<sup>97</sup> Zie: <http://geneva.usmission.gov/2012/07/05/internet-resolution>

<sup>98</sup> Het Rathenau Instituut is nauw betrokken bij de discussies binnen de Raad van Europa. In de zomer van 2013 werd het Rathenau Instituut door het Committee on Bioethics van de Raad van Europa gevraagd om vanuit het perspectief van de mensenrechten te verkennen welke ethische en juridische uitdagingen samenhangen met opkomende technologieën (Van Est et al. 2014). In juni 2016 is het Rathenau Instituut door de Parlementaire Assemblee van de Raad van Europa (PACE) gevraagd om een expertpaper te schrijven over hoe technologische convergentie, kunstmatige intelligentie en robotica mensenrechten beïnvloeden.

<sup>99</sup> De Raad van Europa is in 1949 opgericht om de democratie, de rechtsstaat en de mensenrechten in Europa te bevorderen. De 47 lidstaten die deel uitmaken van de Raad van Europa hebben onder andere het EVRM aanvaard. Via het Europees Hof voor de Rechten van de Mens (EHRM) kunnen individuen, groepen, organisaties en landen een klacht indienen tegen een lidstaat, door een beroep te doen op het EVRM.

nanotechnologie, hersenwetenschappen en informatietechnologie – heeft voor mensenrechten en menselijke waardigheid (Forus 2014).<sup>100</sup> Een van de implicaties van technologische convergentie is dat biomedische technologie niet alleen binnen de medische praktijk, maar ook daarbuiten steeds meer toegepast wordt (Van Est et al. 2014). Dit brengt vragen met zich mee met betrekking tot de handhaafbaarheid van mensenrechten. Zoals gezien in het historisch hoofdstuk is het ethisch toezicht op de toepassing van biomedische technologie in bijvoorbeeld de medische praktijk op tal van manieren geïstitutionaliseerd. Artikel 14 (*Geen selectie op geslacht*) van het verdrag van Oviedo verbiedt bijvoorbeeld sekseselectie voor niet-medische doeleinden.<sup>101</sup> In de medische praktijk zijn er voorzieningen om dit recht op non-discriminatie<sup>102</sup> te waarborgen. In de veefokkerij vindt sekseselectie door middel van het gebruik van *lab-on-a-chip*-technologie al op grote schaal plaats. Het is goed voor te stellen dat deze goedkope en relatief eenvoudige technologie ook commercieel beschikbaar komt in het niet-medische domein. De vraag wordt dan op welke wijze het recht op non-discriminatie gehandhaafd kan worden.

In mei 2015 heeft het Committee on Bioethics de internationale conferentie *Opkomende technologieën en mensenrechten* georganiseerd (Whittall et al. 2015). In het verlengde daarvan nam de Parlementaire Assemblee van de Raad van Europa (PACE) op 24 juni 2015 een resolutie aan over *Technological convergence, artificial intelligence and human rights*.<sup>103</sup> Technologische convergentie, artificiële intelligentie (AI) en robotica worden volgens de resolutie steeds belangrijker voor de maatschappij en behoeven een vroegtijdige discussie over hoe ze mensenrechten en vrijheden beïnvloeden. Zoals hierboven vermeld, gaf PACE in 1991 het startschot voor de totstandkoming van het Verdrag van Oviedo. In de resolutie over artificial intelligence uit 2015 wordt geadviseerd dat PACE een dergelijke rol ook op het gebied van digitalisering zou moeten vervullen, omdat menselijke waardigheid, identiteit, recht op privacy, en vrijheid van gedachten een belangrijke prioriteit zijn. De resolutie lijkt daarmee aan te geven dat PACE een mogelijke verbreding van het werkveld ziet: van bio-ethiek (ethische kwesties gerelateerd aan biotechnologische en biomedische ontwikkelingen) naar ethiek van convergerende technologieën, waarbinnen digitalisering een centrale drijfveer vormt. Een speciale werkgroep binnen PACE gaat deze notie verder onderzoeken en hoopt in maart 2017 met aanbevelingen te komen, waarbinnen binnen de Parlementaire Vergadering over besloten zal worden.

---

<sup>100</sup> Zie ook: [coe.int/en/web/bioethics/emerging-technologies](http://coe.int/en/web/bioethics/emerging-technologies)

<sup>101</sup> Artikel 14 *Geen selectie op geslacht* van het Verdrag van Oviedo stelt "Het gebruik van kunstmatige voortplantingstechnieken om daarmee het cgeslacht van het toekomstige kind te kiezen, is niet toegestaan, behalve ter voorkoming van een ernstige geslachtsgebonden erfelijke aandoening."

<sup>102</sup> Artikel 11 *Non-discriminatie* van het Verdrag van Oviedo luidt "Elke vorm van discriminatie van een persoon op grond van zijn of haar genetisch erfgoed is verboden."

<sup>103</sup> Technological convergence, artificial intelligence and human rights. Motion for a resolution. Doc. 13833, 24 June 2015. Parliamentary Assembly of the Council of Europe. Zie [assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21951&lang=en](http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21951&lang=en)



**Tabel 1** Activiteiten binnen het domein van grond- en mensenrechten.

Wie/wat	Technologie	Issue	Actie
Staatscommissie Thomassen	Digitalisering	Specifiek: vrijheid van meningsuiting, privacy, vertrouwelijke communicatie	Voorstel tot grondwetswijziging art 7, 10, 13
Regering	Digitalisering	Specifiek: vertrouwelijke communicatie	Grondwetswijziging art 13
VN Mensenrechtenraad	Internet	Breed: mensenrechten op het Internet	Internetresolutie L13
VN Mensenrechtenraad	Internet	Specifiek: recht op vrijheid van mening en meningsuiting	Speciale Rapporteur Vrijheid van meningsuiting
VN Mensenrechtenraad	Digitalisering	Specifiek: recht op privacy	Speciale Rapporteur Privacy
UNESCO, IBC	Big data & health	Breed: ethische kwesties	Vorbereiding rapport
UNESCO, COMEST	Robotica	Breed: ethiek van robotisering	Vorbereiding rapport
Parlementaire Assemblée van de Raad van Europa (PACE) motie	NBIC convergentie en artificiële intelligentie; digitalisering	Breed: impact NBIC op mensenrechten	Onderzoek behoefte verbreding werkveld van bio-ethiek naar NBIC-ethiek

## Wetenschap

Het domein van de wetenschap en kennis voedt de maatschappelijke en politiek-bestuurlijke discussie met informatie, concepten en inzichten. De wetenschap draagt bij aan het signaleren en het articuleren van de ethische vraagstukken die de digitalisering oproept. Wetenschappelijke analyses voeden de politiek en bestuur bij het formuleren van een opvatting of het bepalen van een handelingsperspectief. En wetenschap zorgt voor reflectie op het governancestelsel en de uitvoering van beleid. In hoofdstuk 3 hebben we aan de hand van wetenschappelijke literatuur een inventarisatie gemaakt van de ethische vragen die bij digitalisering worden gesignaleerd. In deze paragraaf beschrijven we de rol die wetenschap in het governance-ecosysteem inneemt. Kader 1 geeft een kort overzicht van aanbevelingen en handelingsperspectieven op het gebied van governance, zoals die genoemd worden in de wetenschappelijke literatuur die voor hoofdstuk 3 gebruikt is.

### **Politiek en bestuur**

De wetenschap draagt direct bij het politiek-bestuurlijke proces door in opdracht wetenschappelijke kennis te leveren om politici en beleidsmakers te ondersteunen, bijvoorbeeld in de vorm van studies of wanneer individuele wetenschappers als expert worden geraadpleegd tijdens een hoorzitting of rondetafelgesprek in de Tweede Kamer. Wetenschap speelt vaak een belangrijke rol in de articulatie van concepten. De aanleiding voor de discussie die leidde tot het instellen van de staatscommissie Franken was de dissertatie van Hofman uit 1995 over het begrip 'vertrouwelijke communicatie' (Kamerstukken II 1996-1997, 25 443, nr. 1/2). Ook de betekenis van het concept privacy wordt in sterke mate gevoed door een wetenschappelijke discussie over het begrip (zie bijvoorbeeld Solove 2002). In dit kader is ook het onderzoeksproject van Prof. dr. B.J. Koops naar de betekenis van het begrip privacy in de eenentwintigste eeuw illustratief. Koops wil het privacybegrip opnieuw uitvinden voor een tijdperk waarin, met de opkomst van technologie zoals smartphones en het Internet of Things, het onderscheid tussen de publieke en private ruimte is veranderd (Martijn 2016).

### **Maatschappelijk debat**

Via de media dragen wetenschappers ook bij aan de maatschappelijke discussie. Denk aan het eerder genoemde opiniestuk in de Britse krant *The Guardian* van onder meer Hawking, waarin hij en andere prominente wetenschappers waarschuwen voor de gevaren van artificiële intelligentie (Hawking et al. 2014). Of de studie van Frey en Osborne (2013) die met berekeningen over de automatisering van bepaalde banen het startpunt vormde voor een discussie over de relatie tussen technologie en arbeid. De Amerikaanse Universiteit Stanford bracht recent de eerste uitkomsten van een honderdjarig onderzoek naar de effecten van AI op de samenleving uit, waarin een belangrijke aanbeveling is dat er binnen de overheid meer technologische expertise nodig is om effectief beleid te kunnen maken. Ook in Nederland speelt de wetenschap een belangrijke rol in het aanjagen van het maatschappelijke en het politieke debat. Hoogleraar Computational Social Sciences Helbing stelt in het NRC dat we bouwen aan een dictatuur van data doordat overheden zich steeds meer laten leiden door big data (van Noort 2016). Hoogleraar Global ICT Law Moerel stelt dat het uitleveren van privacy voor korting ervoor zorgt dat privacy alleen nog voor de rijken is (Moerel 2015). En hoogleraar computerbeveiliging Jacobs liet met zijn onderzoeksgroep zien dat de beveiliging van onder andere de OV-chipkaart niet deugde (Radboud Universiteit 2016).

### **Maatschappelijk verantwoorde innovatie**

Naast het voeren van de discussie zorgt de wetenschap ook voor innovaties die een antwoord kunnen geven op maatschappelijke en ethische kwesties, zoals oplossingen op het gebied van privacy by design, of nieuwe cryptografische technieken die het internet veiliger kunnen maken. In onderzoeksfinanciering wordt er vanuit concepten zoals *Responsible Research and Innovation* en *Maatschappelijk Verantwoord Innoveren (MVI)* gedacht over de maatschappelijke meerwaarde van innovatie. Een belangrijk onderdeel van deze filosofie is dat ethische aspecten van innovatie in een vroeg stadium worden geïdentificeerd, en zo kunnen worden meegenomen in een ethisch verantwoorde ontwikkeling van wetenschap en innovatie. In de wetenschapsvisie (Kamerstukken II, 2014-2015, 29338, nr.141) en in de Kamerbrief over ethische aspecten van het innovatiebeleid (Kamerstukken I, 2015-2016, 33009 nr. 16) wordt het MVI-programma van NWO gezien als een belangrijke manier om met de ethische en maatschappelijke vragen omtrent innovatie om te gaan. Daarnaast kijkt de wetenschap ook of zij zelf in het wetenschappelijk onderzoek op een

verantwoorde manier met groeiende dataverzamelingen omgaat. De Koninklijke Nederlandse Academie van Wetenschappen raad aan om een *Ethical Review Board Informatics* in te stellen om te beoordelen of er bij informatica-onderzoek op een verantwoorde manier met persoonlijke gegevens om wordt gegaan.

### **Kader 1: Aanbevelingen in wetenschappelijke literatuur**

In de wetenschappelijke literatuur die in hoofdstuk 3 is gebruikt om een breed palet aan ethische en maatschappelijke aspecten van digitalisering te beschrijven, doen verschillende auteurs ook aanbevelingen over de governance van die aspecten. Een belangrijke taak ligt volgens de wetenschap bij bedrijven, die technologie op zo'n manier kunnen ontwikkelen dat ze op een ethisch verantwoorde manier worden ingezet, het zogeheten *ethics by design*. Het kan daarbij bijvoorbeeld gaan om het inbouwen in de technologie van transparantie, privacybescherming en juridische bescherming. Technologieën kunnen zo worden ontworpen dat waarden zoals privacy en autonomie gewaarborgd blijven, bijvoorbeeld met behulp van speciale encryptiemaatregelen of door de data weer tot iets tastbaars te maken. Bij *digital agents*, zoals robots en AI, geldt dat bedrijven een belangrijke verantwoordelijkheid hebben in het ontwikkelen van technologie dat op een ethisch verantwoorde manier beslissingen neemt. Dit is echter geen eenvoudige opdracht, aangezien het vaak niet eenduidig is wat adequaat ethisch handelen in een bepaalde situatie precies betekent. Daarnaast wordt het belangrijk gevonden flexibiliteit in de technologie in te bouwen. Technologische componenten moeten mee kunnen groeien met de tijd, zodat ze zich kunnen aanpassen aan technologische ontwikkelingen en mogelijk veranderende morele opvattingen.

Burgers moeten volgens een aantal wetenschappers een belangrijkere stem krijgen in het debat over digitalisering en meer inzicht, controle en eigenaarschap krijgen over hun data. Op welke manier dat zou moeten gebeuren en hoe technologie hierbij kan worden ingezet, is iets waar we ons verder over zouden moeten buigen. Hierbij wordt gewezen op de eigen verantwoordelijkheid van burgers, die als gebruiker ook zelf moeten waken over hun data. Op collectief niveau zijn burgers mogelijk zelfs in staat om maatschappelijk ongewenste technologische ontwikkelingen af te remmen, door zelf alternatieven te ontwikkelen of tegenbewegingen in gang te zetten.

Waar het gaat over regulering op het gebied van digitalisering is er behoefte aan zowel breed als specifiek toepasbare regels. Omdat technologische ontwikkelingen ingrijpend kunnen zijn en tegelijkertijd razendsnel gaan, zijn er robuuste regels nodig die snel aangepast kunnen worden. Dit betekent dat er binnen het proces van beleidsbepaling ruimte moet zijn om deze regels regelmatig te evalueren en aan te passen. Andere brede beleidsopties zijn bijvoorbeeld het subsidiëren van initiatieven die specifiek gericht zijn op het waarborgen van maatschappelijke waarden, het stimuleren van de ontwikkeling van nationale en internationale privacy- en transparantiestandaarden voor bedrijven en overheid, en het onderwijzen van burgers over mogelijke risico's en hun eigen verantwoordelijkheid hierbij. Ook wordt er vaak gevraagd om toetsing en toezicht vanuit de overheid, waarmee de

overheid waakt voor bijvoorbeeld de autonomie of de privacy van de burger.

Wellicht vanzelfsprekend pleiten wetenschappers voor meer onderzoek. Dit moet plaatsvinden op verschillende terreinen. Belangrijk is dat er voor zover dit mogelijk is zowel onderzoek wordt gedaan naar de verwachte gevolgen van technologie voor mens en samenleving, als naar de daadwerkelijke gevolgen. Hier moet een ethische analyse van worden gemaakt. Daarnaast is onderzoek nodig naar hoe *digital agents* ethische beslissingen kunnen nemen. Dit vraagt om meer inzicht in de ethiek en in de manier waarop morele opvattingen in de toekomst zouden kunnen veranderen. Verder is er methodologisch onderzoek nodig naar manieren waarop we beter op technologie kunnen anticiperen (bijvoorbeeld door middel van scenariostudies) en hoe we in kunnen grijpen als dat nodig is.

## Maatschappelijke actoren en debat

Maatschappelijke actoren spelen een belangrijke rol in de governance van maatschappelijke en ethische vragen omtrent digitalisering. Bedrijven en technologieontwikkelaars geven vorm aan digitale technologie en maken daarin hun eigen, deels morele, keuzes. Door middel van zelfreguleringsmechanismen zoals interne ethische commissies, gedragscodes en convenanten leggen bedrijven vast hoe zij willen handelen. Maatschappelijke organisaties voeden de politiek-bestuurlijke en maatschappelijke discussie over digitalisering, en kunnen zo ook bijdragen aan bewustwording en wellicht aan digitaal empowerment van het individu. En het individu geeft met zijn eigen keuzes ook vorm aan hoe digitale technologie een plek krijgt in de maatschappij. We geven hier een overzicht van enkele relevante actoren en hun initiatieven. Het overzicht is niet volledig, maar bedoeld om een beeld te schetsen van het type acties dat door maatschappelijke actoren wordt genomen.

### ECP Platform voor de informatiesamenleving

Stichting ECP is een organisatie met als missie het ondersteunen van een betrouwbare, kansrijke digitale samenleving in Nederland. ECP is onafhankelijk en acteert als verbinder en aanjager tussen publieke en private partijen zoals ministeries, telecombedrijven en maatschappelijke organisaties zoals de Consumentenbond. Met projecten, evenementen, onderzoek en debat zet ECP het maatschappelijke en economische belang van digitalisering op de agenda. Een belangrijke pijler van het werk van ECP is het stimuleren en verbeteren van digitale veiligheid, zowel bij bedrijven, overheden en individuele burgers. ECP was in de afgelopen jaren betrokken bij verschillende programma's over veilig online gedrag, zoals de campagne AlertOnline, het programma Digivaardig Digiveilig en de site Veilig Internetten waar gebruikers bijvoorbeeld informatie kunnen vinden over hoe ze veilig kunnen omgaan met online privacy en wachtwoorden. Ook zit ECP het Platform Internetveiligheid voor waarin strategisch overleg tussen private en publieke partijen over hoe internetveiligheid te bevorderen.

Een andere belangrijke pijler in de activiteiten van ECP is het stimuleren van digitale vaardigheden. Dat gebeurt door middel van bewustwording – bijvoorbeeld in de campagnes over internetveiligheid

– maar ook door activiteiten gericht op het leren programmeren, zoals het CodePact. Het doel van het CodePact is om zoveel mogelijk kinderen de kans te bieden te leren programmeren, daartoe worden er onder andere programmeerlessen georganiseerd tijdens de jaarlijkse Codeweek. ECP start in 2015 de werkgroep Ethiek en Informatiesamenleving, die zich buigt over de ethische dilemma's waar techniek en digitalisering ons voor plaatsen. Eind 2016 volgt een essaybundel over het onderwerp.<sup>104</sup> Met het visiedocument *De volwassen informatiesamenleving* bepleit ECP tot slot een discussie over ethiek, niet vanuit een tegenstelling tussen mens en technologie, maar vanuit de erkenning dat de mens een technologisch wezen is (ECP 2015).

### **Bits of Freedom**

Stichting Bits of Freedom is een digitale burgerrechtenbeweging, die zich sinds 1999 richt op het beschermen van vrijheid en privacy op het internet. Privacy en communicatievrijheid zijn volgens Bits of Freedom twee grondrechten die onmisbaar zijn voor de individuele ontplooiing en de democratie. De stichting zet zich met behulp van campagnes en lobby's in voor deze waarden en probeert ervoor te zorgen dat 'overheid en bedrijfsleven slecht beleid terugdraaien en goed beleid invoeren'.

Een van de bekendste campagnes is de jaarlijkse uitreiking van de Big Brother Awards. Deze worden uitgereikt aan bedrijven of overheidsorganisaties die zich schuldig hebben gemaakt aan privacyschendingen. In 2013 ontving de toenmalig minister van Veiligheid en Justitie Ivo Opstelten een Big Brother Award, hetgeen aanleiding was voor het stellen van Kamervragen door de leden Schouw en Verhoeven (Handelingen 2013-2014, 211). In 2015 kreeg minister Plasterk van Binnenlandse Zaken en Koninkrijksrelaties een Big Brother Award voor het wetsvoorstel voor de nieuwe Wet op de inlichten en veiligheidsdiensten (Wiv). Bits of Freedom laat ook in diverse wetgevingstrajecten van zich horen. In de internetconsultatie voor de Wiv schreef de stichting een reactie en werd een speciale website ontworpen die toegankelijke uitleg gaf bij de wetsteksten en het makkelijker maakte voor burgers en organisaties om op het wetsvoorstel te reageren.

Als initiatiefnemer van de Privacycoalitie van 32 partijen, roept Bits of Freedom in 2015 de minister van Veiligheid en Justitie op een visie te ontwikkelen op privacybescherming.<sup>105</sup> De minister zou hiertoe een publiek debat moeten faciliteren en wordt gevraagd de behandeling van nieuwe wetten die een impact hebben op de privacy op te schorten totdat er daadwerkelijk een duidelijke visie is. De minister nodigde de Privacycoalitie uit voor een gesprek over de oproep, waarin de toetsstenen van het kabinet op het gebied van privacybescherming worden toegelicht (Kamerstukken II 2013-2014, 32761, nr. 83). De minister gaat niet in op de eis de behandeling van wetsvoorstellen op te schorten. Wel zegt hij toe de Privacycoalitie ook in een toekomstige dialoog over het onderwerp privacy te betrekken, bijvoorbeeld bij de kabinetsreactie op het WRR-rapport over big data (WRR 2016).

---

<sup>104</sup> Zie voor meer informatie de jaarverslagen van ECP via [ecp.nl/jaarverslag](http://ecp.nl/jaarverslag)

<sup>105</sup> De oproep wordt onder andere ondertekend door Nederlandse Vereniging van Juristen, SETUP, Privacy First, Open State Foundation, Stichting Digitale Infrastructuur Nederland (DINL), Waag Society, Publeaks, Kennisland, Privacy Barometer, Internet Society Nederland (ISOC.nl). Zie voor een volledig overzicht [bof.nl/2015/04/02/persbericht-brede-coalitie-vraagt-visie-privacybescherming-ard-van-der-steur](http://bof.nl/2015/04/02/persbericht-brede-coalitie-vraagt-visie-privacybescherming-ard-van-der-steur)

Tot slot probeert Bits of Freedom digitale vaardigheden en bewustwording bij een breed publiek te stimuleren. Zo werd de Internetvrijheid Toolbox gelanceerd waarmee gebruikers praktische adviezen, tips en links naar applicaties krijgen om hun privacy, vertrouwelijke communicatie, en gegevensbeveiliging mee te versterken. Door middel van projecten in samenwerking met journalistiek media geeft de stichting inzicht in bijvoorbeeld de praktijken van data-handelaren in Nederland, of de Nederlandse lobby met betrekking tot de Europese Algemene verordening gegevensbescherming (Bits of Freedom 2015).

### **Privacy First**

De stichting Privacy First is in 2008 opgericht als onafhankelijke stichting ter behoud en bevordering van het recht op privacy. Het probeert privacyschendingen via politieke lobby, publiekscampagnes of juridische acties en rechtszaken tegen te gaan. Belangrijke onderwerpen zijn in de afgelopen jaren biometrie, cameratoezicht, de OV-chipkaart, medische privacy, mobiliteit en anonimiteit in de openbare ruimte (Privacy First 2015). Vaak is de overheid bij die onderwerpen het punt van aandacht, al stelt de stichting zich de komende jaren ook meer te willen richten op bedrijven.

Juridische procedures vormen een belangrijk middel waarmee Privacy First optreedt tegen privacyschendingen. De stichting spant procedures aan over de opslag van vingerafdrukken onder de Paspoortwet, het kentekenparkeren, trajectcontroles, en de Wet bewaarplicht telecomgegevens (Wbt). Met betrekking tot de Wbt oordeelde de rechtbank Den Haag in 2015 dat de wet in strijd is met het recht op privacy en buiten werking moet worden gesteld.<sup>106</sup> Deze uitspraak is in lijn met het oordeel van het Europees Hof van Justitie over de vrijwel identieke Europese Databetrouwelijkheidsrichtlijn. In de juridische procedures werkt Privacy First samen met advocatenkantoren, maatschappelijke organisatie, zoals het Nederlands Juristen Comité voor de Mensenrechten (NJCM), en soms ook met individuele burgers. Daarnaast probeert de stichting ook individuele burgers die met vragen over privacybescherming zitten zo goed mogelijk van informatie te voorzien. Incidenteel worden individuele juridische cases van burgers geadopteerd of ondersteund, maar de stichting geeft aan hier weinig capaciteit voor te hebben (Privacy First 2015).

Tot slot wordt met het initiatief Privacy First Solutions sinds 2014 getracht om privacyvriendelijk handelen bij overheid en bedrijfsleven onder de aandacht te brengen. Bijvoorbeeld door het stimuleren van de toepassing van *privacy by design* en het toekennen van prijzen voor privacyvriendelijke diensten en producten (Privacy First 2015).

### **Consumentenbond**

De Consumentenbond is een onafhankelijke vereniging die zich inzet voor het belang en de rechten van consumenten, door middel van campagnes, acties, onderzoek en informatievoorziening. De consumentenbond houdt zich ook bezig met de privacy van consumenten. Uit eigen onderzoek blijkt dat 54 procent van de consumenten de privacyvoorwaarden soms of zelden leest, terwijl 95 procent bescherming van privégegevens (zeer) belangrijk vindt. De bond heeft van diverse producten, waaronder elf bekende Nederlandse Android-apps, de voorwaarden tegen het licht

---

<sup>106</sup> Eisers in deze zaak waren Stichting Privacy First, de Nederlandse Vereniging van Strafrechtadvocaten (NVSA), de Nederlandse Vereniging van Journalisten (NVJ), het Nederlands Juristen Comité voor de Mensenrechten (NJCM), internetprovider BIT en telecomaانبieders VOYS en SpeakUp, een en ander onder leiding van Boekx Advocaten in Amsterdam.

gehouden. Volgens de Consumentenbond zijn de voorwaarden vaak veel te vaag en wordt de consument slecht geïnformeerd. De consumentenbond helpt via een stappenplan gebruikers de privacyinstellingen op hun mobiele telefoons beter te beheren. De bond levert ook kritiek op de privacyvoorwaarden van tal van slimme TV's, die in reactie hierop door leveranciers werden aangepast. Naar aanleiding van onderzoek naar dating- en fitnessapps van de Noorse consumentenbond dringt de Nederlandse consumentenbond, samen met Noorwegen, Zweden en Slovenië aan op betere voorwaarden bij de makers van dergelijke apps.<sup>107</sup>

Met de campagne Digidwang verzet de Consumentenbond zich ertegen dat steeds meer organisaties consumenten dwingen tot digitalisering. De bond komt daarmee op voor de belangen van consumenten die niet mee kunnen of mee willen gaan in de digitalisering. Met de campagne Digidwang spreekt ze zich uit tegen voornemens van onder andere de Belastingdienst om op termijn alleen nog digitale post te versturen. Iedereen moet volgens de Consumentenbond kunnen kiezen op welke wijze hij of zij wordt benaderd. Ook de Nationale ombudsman, de FNV en de ouderenbonden Unie KBO, ANBO (een belangenorganisatie voor senioren) en PCOB (een christelijke ouderenorganisatie) spreken zich uit tegen digitaliseringsdwang. De komende jaren wil de Consumentenbond zich richten op de handel in persoonsgegevens en de negatieve effecten die dat kan hebben, zoals het ontstaan van 'risicoprofielen' die aan mensen worden gekoppeld. Op dit moment ontvangt de Consumentenbond tientallen meldingen per jaar van datadiscriminatie; mensen die door een 'moeilijk' dataprofiel zijn geweigerd of een toeslag moeten betalen. De Consumentenbond gaat bovendien uitzoeken waar oneigenlijk en te veel gegevens worden verzameld of gedeeld met derden, en waar nodig bedrijven aanspreken op oneigenlijk verzamelen of delen van gegevens.

### **Enkele overige maatschappelijke organisaties**

Verschillende andere maatschappelijke organisaties houden zich op meer of minder structurele wijze bezig met ethische en maatschappelijke kwesties omtrent digitalisering. We noemen slechts enkele organisaties. De Nederlandse Juristen Vereniging bracht in het afgelopen jaar het pre-advies Homo Digitalis uit, waarin de impact van digitalisering op het recht en vanuit juridisch perspectief bezien wordt (NJV 2016). Het Nederlands Juristen Comité voor de Mensenrechten (NJCM) zet zich in voor de bescherming van mensenrechten in Nederland. Het NCJM levert commentaren op wetsvoorstellen zoals de herziening van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) waarin ze schendingen van privacy aan de kaak stelt. De ANWB lanceert samen met haar Europese zusterorganisaties de campagne *My car, my data* om het publiek bewust te maken en regelgeving te bepleiten over de data die fabrikanten van slimme auto's verzamelen. Het SIDN Fonds stimuleert jaarlijks initiatieven die het internet beogen te versterken, de positie van gebruikers te verstevigen, en de maatschappelijke meerwaarde van het internet te verhogen.<sup>108</sup> Stichting NLNet ondersteunt personen en organisaties (zoals Bits of Freedom) die bijdragen aan het versterken en het beschermen van een open en vrij internet. Verschillende culturele organisaties zoals V2\_, Waag Society en SETUP zorgen met workshops, lezingen en exposities

<sup>107</sup> Zie Consumentenbond (2015) en [consumentenbond.nl/campagnes/privacy](http://consumentenbond.nl/campagnes/privacy)

<sup>108</sup> [sidnfonds.nl/wat-we-doen](http://sidnfonds.nl/wat-we-doen)

voor een kritische reflectie op digitalisering vanuit het culturele domein, en dragen met hun activiteiten bij aan het versterken van digitale vaardigheden bij het algemeen publiek.

### Bedrijfsleven

Op het gebied van privacy zijn er verschillende bedrijven die zich profileren door het leveren van privacyvriendelijke diensten. Voorbeelden zijn de QIY foundation die werkt aan een systeem dat gebruikers meer controle over hun eigen data geeft. De zoekmachine Ixquick biedt mensen een mogelijkheid om te zoeken op het web zonder daarbij persoonlijke gegevens af te staan. Internet providers zoals XS4All en Greenhost zetten zich in voor een open en vrij internet en digitale veiligheid. Ook zijn er vanuit bedrijfstakken initiatieven op het gebied van privacy. Zo sloot het Verbond van Verzekeraars met haar leden een convenant af over gegevensbescherming. Recent bracht het Verbond een greenpaper *Grip op data* uit waarin de effecten van digitalisering voor de sector worden geanalyseerd, en een solidariteitsmonitor wordt aangekondigd om in de gaten te houden hoe data maatschappelijke solidariteit beïnvloed (Verbond van Verzekeraars 2016). Ondernemingsorganisatie VNO-NCW maakt zich samen met MKB Nederland hard voor meer aandacht voor digitale veiligheid.<sup>109</sup> Verder zijn er ook binnen bedrijven structuren waarin over de ethische aspecten van digitalisering wordt nagedacht. Zo heeft de Rabobank een Commissie Ethiek en een Bureau Ethiek, waarin ook het onderwerp digitalisering aan de orde komt.<sup>110</sup>

De verantwoordelijkheid van bedrijven om mensenrechten te respecteren is in de Richtlijnen voor Multinationale Ondernemingen van de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO-richtlijnen) opgenomen.<sup>111</sup> De OESO-richtlijnen nemen het concept van *due diligence* uit de *United Nations Guiding Principles on Business and Human Rights* (UNGP's)<sup>112</sup> over. Daaronder wordt het proces verstaan waarmee ondernemingen daadwerkelijke en potentiële negatieve effecten van hun activiteiten kunnen identificeren, voorkomen en verminderen, en waarmee zij verantwoording kunnen afleggen over hun aanpak van die effecten als integraal onderdeel van hun besluitvormingsproces en risicobeheerssystemen. Bedrijven dienen zich actief in te spannen om risico's op schendingen van mensenrechten door henzelf of partijen in hun keten te onderkennen en waar mogelijk schendingen te voorkomen. Meldingen over vermeende schendingen van de OESO-richtlijnen kunnen worden gedaan bij het Nationaal Contactpunt (NCP). Tot op heden zijn er echter nog geen meldingen bij het Nationaal Contactpunt gedaan in verband met digitalisering.<sup>113</sup>

<sup>109</sup> vno-ncw.nl/nieuws/versnelling-aanpak-cybersecurity-hard-nodig

<sup>110</sup> Interview Françoise Rost 22-04-2016

<sup>111</sup> OESO principes voor Multinationals (OESO 1976; 2011) over bedrijfsethische kwesties en verantwoordelijke bedrijfscodes. De Nederlandse overheid heeft deze richtlijnen onderschreven; zij verwacht van bedrijven dat ze maatschappelijk verantwoord ondernemen (TK 2012-2013).

<sup>112</sup> De UNGP's zijn ontwikkeld onder leiding van VN-Speciaal Vertegenwoordiger John Ruggie (daarom ook wel Ruggie principes genoemd). De principes bestaan uit drie pijlers. De eerste pijler herbevestigt de plicht van staten om mensenrechten te beschermen. De tweede pijler is gericht op de verantwoordelijkheid van bedrijven om mensenrechten te respecteren. De derde pijler betreft de noodzaak om slachtoffers van mensenrechtenschendingen door activiteiten van bedrijven mogelijkheden te geven op herstel en/of genoegdoening (Kamerstukken II 2015-2016, 26485, nr. 219). De UNGP's leggen geen juridische verplichtingen op maar vormen een gezaghebbende internationale standaard.

<sup>113</sup> oesorichtlijnen.nl/meldingen. De OESO MVO richtlijnen gaan uit van mensenrechten zoals beschreven in de Universele Verklaring van de Rechten van de Mens.



Op initiatief van de Europese Commissie stellen lidstaten op nationaal niveau plannen op om de UNGP's te implementeren. In Nederland is dat het Nationaal Actieplan Bedrijfsleven en Mensenrechten (NAP) uit 2013 (Kamerstukken II 2012-2013, 26485, nr. 174). Eén van de actiepunten in het NAP is nader onderzoek naar de regulering van de zorgplicht van Nederlandse bedrijven. Dit onderzoek is in 2016 afgerond. Een van de aandachtspunten is: 'de praktische en procedurele drempels voor het aansprakelijk stellen van bedrijven, zoals hoge kosten, bewijsproblemen en beperkingen in de mogelijkheden collectieve acties in te stellen' (Kamerstukken II 2015-2016, 26485, nr. 219). Het kabinet geeft aan dat bij de herziening van het civiel bewijsrecht en bewijslast het zorgplichtonderzoek wordt meegewogen.

Om beschikbare informatie over *due diligence* voor bedrijven toegankelijk te maken, heeft de Europese Commissie voor drie sectoren *Sector Guidances* op laten stellen, waaronder voor ICT (EC 2011). Deze handleidingen geven bedrijven advies hoe ze hun verantwoordelijkheid om mensenrechten te respecteren in de alledaagse bedrijfsvoering kunnen implementeren.

### **Internationale ontwikkelingen**

Op internationaal vlak is een levendige discussie over de ethiek van digitalisering zichtbaar. Verschillende organisaties en personen hebben opgeroepen tot digitale rechten, nieuwe vormen van bescherming, ethische commissies en gedragscodes. Wetenschapper Hawking, Tesla-voorman Musk en Apple-oprichter Wozniak schaarden zich achter een oproep tot een verbod op autonome wapens (Future of Life Institute 2015). Berners Lee, de grondlegger van het wereldwijde web, deed een oproep tot een digitale Magna Carta, om de rechten van internetgebruikers te beschermen (Kiss 2014). Ter ere van de 800ste verjaardag van de Magna Carta lanceerde de British Library een crowdsourcinginitiatief waarin – in reactie op de oproep van Berners-Lee voor een Magna Carta voor het web – mensen hun suggesties voor een digitale Magna Carta konden inbrengen.<sup>114</sup>

Niet alleen organisaties spelen een rol in de maatschappelijke discussie over digitalisering. In de afgelopen jaren zijn er ook enkele individuele burgers geweest die met hun onthullingen of acties een maatschappelijk debat hebben aangejaagd. De onthullingen van klokkenluider Snowden leidden tot veel maatschappelijke en politieke discussie over dataverzameling en surveillance door de overheid. De Oostenrijkse privacyactivist Schrems baarde opzien door een twaalfhonderd pagina's tellend document van persoonlijke gegevens bij Facebook op te vragen, en wist met een procedure bij het Hof van Justitie van de Europese Unie ervoor te zorgen dat het *Safe Harbour*-besluit (2000/520/EC) – dat gegevensuitwisseling tussen Europa en de Verenigde Staten regelde – ongeldig werd verklaard. Hierdoor werd de Europese Commissie aangezet om tot een nieuwe overeenkomst te komen waarin gegevens van Europese burgers beter woerden beschermd bij uitwisseling met bedrijven in de VS.

Vaak is er een sterke interactie tussen de acties van de maatschappelijke actoren en de initiatieven die in het politiek-bestuurlijke domein plaatsvinden. De discussie over digitale rechten die onder andere door de oproep van Berners-Lee wordt aangewakkerd, leidde in het Verenigd Koninkrijk,

---

<sup>114</sup> [bl.uk/my-digital-rights](http://bl.uk/my-digital-rights)

zoals in paragraaf 5.5 beschreven tot politieke initiatieven om te komen tot een Digital Bill of Rights. Het European Digital Rights Initiative (EDRi) lanceerde met andere burgerrechtenorganisaties, zoals Bits of Freedom, een campagne in de aanloop naar de Europese verkiezingen in 2014. Met de campagne We Promise werd kandidaten voor het Europees Parlement gevraagd zich te houden aan een verdrag van tien principes om digitale rechten te beschermen (EDRi 2014).

In 2014 namen een Britse en een Canadese denktank het initiatief om een internationale commissie op te richten om een toekomstvisie op internet governance te ontwikkelen. De Global Commission on Internet Governance (GCIG) bestaat uit 29 stakeholders. In 2016 komt de commissie met een aantal aanbevelingen om het internet toegankelijk, open, veilig en betrouwbaar te houden (GCIG 2016). De fundamentele rechten van digitale burgers, zoals privacy en vertrouwelijke communicatie, moeten worden beschermd, overheden moeten bedrijven niet dwingen om technische achterdeurtjes in software in te bouwen, beslissingen door algoritmen moeten kunnen worden gecontroleerd en producenten van software en digitale diensten moeten aansprakelijk zijn voor de kwaliteit van de technologie die ze produceren.

In 2016 riep de Britse innovatiestichting Nesta op een *Machine Intelligence Commission* op te richten (Mulgan 2016). Een dergelijke commissie is volgens Nesta nodig om het publieke belang te beschermen bij de inzet van algoritmen en kunstmatige intelligentie en het publiek vertrouwen te behouden. Volgens Nesta zou de commissie geen formele rol moeten hebben in het certificeren of goedkeuren van algoritmen, maar sterke bevoegdheden om onderzoek te verrichten en toegang tot informatie te krijgen. Goede technische vaardigheden en de mogelijkheden om zelf software te ontwikkelen om computersystemen te bevragen, zijn daarbij van belang. De commissie zou naar toepassingen in verschillende belangrijke sectoren moeten kijken – zoals gezondheid, mobiliteit, financiën – en aanbevelingen doen aan diverse handhavingsautoriteiten. Nesta baseert de aanbevelingen op de ervaringen met eerdere commissies in het Verenigd Koninkrijk omtrent milieuvervuiling en embryo-gebruik. Dergelijke commissies hebben een belangrijke rol gespeeld in het stimuleren van maatschappelijk debat over ethische grenzen, het creëren en borgen van publiek vertrouwen, en het mogelijk maken van economische ontwikkeling (Mulgan 2016).

Tot slot zijn er ook initiatieven die zich direct op de ontwikkeling van technologie richten. De Internet Engineering Taskforce (IETF), die Internetprotocollen en -standaarden ontwikkelt, heeft recent een Human Rights Protocol Considerations Research Group (HRPC) opgericht samen met de mensenrechtenorganisatie Article 19. De groep onderzoekt hoe rekening kan worden gehouden met mensenrechten bij het ontwerp van de protocollen en standaarden van het web (Ten Oever & Cath 2016). Het Institute of Electrical and Electronics Engineers (IEEE), de internationale organisatie voor technische professionals, lanceerde een initiatief om methoden voor ethiek bij het ontwerp van autonome systemen te ontwikkelen (IEEE 2016). De eerste stap wordt gezet door een verzameling van de meest significante ethische vraagstukken te maken met behulp van de community van het IEEE en hierop aanbevelingen te formuleren. Dit moet leiden tot een levend document dat ontwerpers helpt ethisch verantwoorde keuzes te maken bij het maken van autonome systemen. Ook bij sommige bedrijven worden commissies ingesteld om met ethische vragen om te gaan. Google stelde in 2004 een Ethics Board in, die zich onder meer bezighoudt met kunstmatige intelligentie. Over de rol en de samenstelling van de commissie wordt echter vrijwel niets naar buiten gebracht (Shead 2016). In reactie op de publieke verontwaardiging die Facebook ten deel

kwam na het experiment waarin de emoties van gebruikers werden beïnvloed, stelde het bedrijf een ethische toetsingscommissie in, die onderzoek van het bedrijf op het sociale netwerk vanuit ethisch perspectief gaat beoordelen (Boka 2016).

**Tabel 2** Activiteiten op maatschappelijk niveau

Wie / wat	Technologie	Issue	Actie
ECP	Digitalisering	Veiligheid, privacy, inclusiviteit	Programma's voor digitale skills en veiligheid, werkgroep ethiek & ICT
Bits of Freedom	Internet, digitale communicatie	Privacy, veiligheid	Big brother awards, privacycoalitie, internetvrijheid toolbox
Privacy First	Digitale communicatie, digitale overheid	Privacy	Juridische acties
Consumentenbond	Apps, consumententechnologie	Privacy	Campagne privacybewustzijn. Aanspreken producenten op privacy
OESO-richtlijnen maatschappelijk verantwoord ondernemen	Specifiek case by case	Specifiek case by case	Bedrijven hebben een zorgplicht om mensenrechten te respecteren
<i>EU en internationaal</i>			
EDRi (EU)	Internet, digitale communicatie	Mensenrechten online	Campagne om belofte voor bescherming digitale rechten van parlements kandidaten
Nesta (VK)	AI, algoritmen, robotica	Autonomie, controle over technologie, vertrouwen	Oproep tot een Machine Intelligence Commission
Global Commission on Internet Governance (int.)	Internet, digitale communicatie	Mensenrechten online	Rapport met oproep tot bescherming digitale rechten
IETF (int.)	Internet, digitale communicatie	Mensenrechten	Human Rights Research Group die onderzoekt hoe in protocollen rekening gehouden kan worden met rechten

IEEE (int.)	AI, algoritmen, robotica	-	Initiatief om ontwerpers van autonome systemen te helpen ethische keuzes te maken
-------------	--------------------------	---	---

Rathenau Instituut

## Agendavorming

Op het gebied van agendavorming spelen verschillende adviesraden en instituten een rol. We bespreken slechts die organisaties die ethische en maatschappelijke issues signaleerden op het terrein van digitalisering. Adviezen die wel aandacht besteden aan digitalisering, maar bijvoorbeeld vooral naar de financieel-economische of technische kant kijken laten we buiten beschouwing.<sup>115</sup> Ons overzicht kan niet compleet zijn. Hieronder bespreken we achtereenvolgens enkele nationale activiteiten van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR), de Adviesraad Internationale Vraagstukken (AIV), Raad voor de leefomgeving en infrastructuur (Rli) en het Rathenau Instituut. Op Europees niveau is er aandacht voor de European Group on Ethics in Science and New Technologies.

### Wetenschappelijke Raad voor het Regeringsbeleid

De Wetenschappelijke Raad voor het Regeringsbeleid is een onafhankelijk adviesorgaan met als taak 'wetenschappelijke gefundeerde informatie te verschaffen over ontwikkelingen die op langere termijn de samenleving kunnen beïnvloeden'.<sup>116</sup> De WRR bracht in de afgelopen jaren een aantal rapporten uit waarin diverse ethische en maatschappelijke uitdagingen omtrent digitalisering zijn belicht. Er is gekeken naar digitalisering van de overheid (2011), publieke waarden in het internet (2015), robotisering en werk (2015) en big data (2016).

Het rapport *iOverheid* (WRR 2011) beschrijft hoe digitalisering de overheid fundamenteel verandert. ICT is niet alleen een middel waarmee de overheid haar taken uitvoert, het verandert ook de manier waarop taken en processen worden georganiseerd. Dit zorgt voor nieuwe uitdagingen op het gebied van privacy, transparantie van overheidsprocessen, controle en correctie van vervuilde informatie en de weerbaarheid van burgers. De WRR beveelt daarom onder andere aan tot de oprichting van een iPlatform om transparantie te versterken en een iAutoriteit die de burger bijstaat in problemen met de iOverheid. In 2015 wordt er met het rapport *De publieke kern van internet* (WRR 2015) gekeken naar diverse vraagstukken die samenhangen met het feit dat internet van steeds groter belang is: cybercrime, kwetsbaarheid van vitale infrastructuren, toenemende grip van staten en regulering op internet. De WRR bepleit om het internet tot speerpunt van het buitenlands beleid te verheffen en de publieke kern van het internet vast te leggen in internationale verdragen. Het rapport *De robot de baas* (WRR 2015) onderzoekt de effecten van robotisering op de

<sup>115</sup> Adviezen van bijvoorbeeld de Adviesraad Wetenschap en Technologie (AWTI) het Centraal Planbureau (CPB), Planbureau voor de Leefomgeving (PBL) of Sociaal Cultureel Planbureau (SCP) vallen hierdoor buiten deze beschouwing.

<sup>116</sup> Instellingswet WRR, art. 2.a 30 juni 1976

arbeidsmarkt, en bepleit een inclusieve robotagenda die de complementaire samenwerking tussen mens en machine bevordert en het scenario van technologische werkeloosheid tegengaat. In 2016 brengt de WRR op aanvraag van de ministeries van Veiligheid en Justitie en Binnenlandse Zaken en Koninkrijksrelaties het advies uit over big data in het veiligheidsdomein. De WRR constateert een mismatch tussen big data en huidige wet- en regelgeving. De nadruk in regulering ligt nu op het verzamelen van data. Dit zou aangevuld moeten worden met regulering en toezicht op de analyse en gebruik van big data. De WRR beveelt onder ander aan een zorgplicht in te voeren voor gegevensverwerkende partijen om duidelijk te maken hoe zij tot bepaalde uitkomsten komen. Daarnaast dienen de capaciteiten en technische expertise van toezichthouders, zoals de Autoriteit Persoonsgegevens en de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), versterkt te worden (WRR 2016).

### **Adviesraad Internationale Vraagstukken (AIV)**

De Adviesraad Internationale Vraagstukken (AIV) is een onafhankelijk adviesorgaan dat de regering en het parlement adviseert over het buitenlandse beleid met betrekking tot onder andere veiligheid, vrede en mensenrechten. Op aanvraag van de regering bracht de AIV in 2014 advies uit over internetgovernance en in 2015, samen met de Commissie van Advies inzake Volkenrechtelijke Vraagstukken (CAVV), een advies over autonome wapens.

In de context van internationale internetgovernance, gaat het AIV-advies *Het internet: een wereldwijde vrije ruimte met begrensde staatsmacht* (AIV 2014) in op vraagstukken zoals privacy, informatieveiligheid en surveillance. Nederland dient een actieve rol in te nemen in het beschermen van internetvrijheid, ook in relatie tot bedrijven die hierin een bepalende rol spelen. Daarvoor is een coherente visie op het internet en een sterkere interdepartementale coördinatie nodig. Nederland dient een voorbeeld voor het buitenland te zijn door nationaal een hoog beschermingsniveau van mensenrechten uit te dragen. Daarvoor is het noodzakelijk om kritisch te kijken naar waarborgen bij de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) en toezicht vanuit het Autoriteit Persoonsgegevens (AP) en de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) te versterken.

In het AIV/CAVV-advies *Autonome wapensystemen* (2015) staan de thema's veiligheid en controle over technologie centraal. De instanties stellen dat autonome wapensystemen samen moeten gaan met 'betekenisvolle menselijke controle'. Dat houdt in dat mensen in staat moeten zijn om een geïnformeerde en bewuste keuze te kunnen maken over het gebruik van wapens en het inzetten van (dodelijk) geweld. Een moratorium of verbod op (volledig) autonome wapens wordt niet haalbaar en wenselijk geacht. Autonome wapensystemen dienen te voldoen aan het internationale oorlogsrecht. Daarnaast is het volgens de AIV en CAVV technisch gezien onwaarschijnlijk dat er de komende twintig jaar wapens zullen zijn die kunnen functioneren zonder 'betekenisvolle menselijke controle'. Wanneer in de toekomst door verdere ontwikkeling van kunstmatige intelligentie wapens zo zelfstandig worden dat er geen sprake meer is van betekenisvolle menselijke controle, moeten dergelijke wapens niet worden ingezet.

### **Raad voor de leefomgeving en infrastructuur (Rli)**

De Raad voor de leefomgeving en infrastructuur (Rli) adviseert de regering en het parlement over beleidsvraagstukken die te maken hebben met de duurzame ontwikkeling van de leefomgeving en

infrastructuur. De Rli houdt zich daarmee niet vanzelfsprekend bezig met digitalisering, maar waar het thema een raakvlak heeft met de leefomgeving – zoals in de ontwikkeling van slimme steden of de rol van digitale infrastructuur in het Nederlands vestigingsklimaat – staat het op de agenda.<sup>117</sup>

Met de *Verkenning technologische innovaties in de leefomgeving* (2015b) signaleert de Rli dat de snelle ontwikkeling van technologie grote invloed heeft op onze manier van leven en op morele waarden zoals privacy en transparantie, nog voordat daar goed over na is gedacht. De data-infrastructuur is van steeds groter maatschappelijk en economisch belang. De overheid moet het publieke belang van toegang, transparantie, veiligheid, privacy en robuustheid behartigen. Denk aan redundantie in de data-infrastructuur om lokale uitval op te vangen of aan kwetsbaarheid door afhankelijkheid van een of enkele grote marktpartijen. Met betrekking tot het gebruik van data merkt de raad op dat ook autonomie en de bescherming van keuzevrijheid van groot belang zijn. De technologische ontwikkelingen vragen volgens de Rli om een kabinetbrede visie. De Rli ziet een taak voor de overheid om brede maatschappelijke debatten te organiseren over de impact van technologische innovaties op onze waarden.

### **Rathenau Instituut**

Het Rathenau Instituut speelt een rol in het proces van signalering en beleidsagendering. Als onderzoeksinstituut van de Koninklijke Nederlandse Academie van Wetenschappen heeft het de taak om de publieke en politieke meningsvorming over wetenschap en technologie te stimuleren. Het onderwerp digitalisering is in de afgelopen jaren in een groot aantal verschillende rapporten van het instituut belicht. Ontwikkelingen zoals het Internet of Things, robotica, biometrie, slimme mobiliteit, big data, digitale platformen, en digitalisering in de gezondheidszorg, verzekeringswereld en het boerenbedrijf zijn aan de orde gekomen.<sup>118</sup>

Het thema privacy komt veelvuldig terug, bijvoorbeeld als het gaat over mobiliteit, verzekeren, e-health en big data en het Internet of Things. Nieuwe technologie maakt nieuwe vormen van monitoring mogelijk – bijvoorbeeld van rij- en gezondheidsgedrag of levensstijl – en dat roept vragen op over hoe er met de data wordt omgegaan die via die monitoring verkregen wordt. Het rapport *Voorgeprogrammeerd* (Van 't Hof et al. 2012a) signaleert dat het daarbij niet alleen gaat over het reguleren van het verzamelen van data, maar ook over de analyse en toepassing van data, bijvoorbeeld hoe sociale media en zoekmachines informatie voorsorteren. Dergelijke ontwikkelingen zetten online de keuzevrijheid onder druk (Van 't Hof et al. 2012b). Het Rathenau Instituut pleit voor meer transparantie en bewustwording over profilering. De opkomst van het Internet of Things maakt het bovendien moeilijk voor de consument om al zijn datastromen te managen en controleren, en vraagt zodoende om een nieuwe benadering van privacy (Eskens et al. 2016) waarin bedrijven meer verantwoordelijkheid nemen en er ook oog is voor het recht niet te weten en niet gemeten, geanalyseerd of gecoacht te worden (Van Est 2014). Daarmee schuift de discussie op van informatiele privacy in de zin van bescherming van en controle op persoonlijke gegevens, richting privacy als een grondrecht, gericht op bescherming van de persoonlijke levenssfeer. De grote

---

<sup>117</sup> Zie bijvoorbeeld het werkprogramma van de Rli (2015a; 2016)

<sup>118</sup> Beyond control: Consumer privacy in the Internet of Things (2016), Digitalisering van dieren (2016), De meetbare mens (2016), Verzekeren in de data-gedreven samenleving (2015), Dicht op de huid (2015), De data-gedreven samenleving (2015), De Kracht van platformen (2014), Tem de robotauto (2014), Intieme technologie (2014), Voorgeprogrammeerd (2012), Overall robots (2012)

uitdaging is om privacy in die originele mensenrechtelijke zin te blijven waarborgen in een steeds verder digitaliserende samenleving.

Een terugkerende dynamiek in de rapporten is het toetreden van nieuwe partijen die de bestaande markt – het medische domein, het mobiliteitsdomein, de verzekeringspraktijk, of de landbouwwereld – opschudden met vernieuwende data-gestuurde verdienmodellen. Daarmee worden ook allerlei ICT-vraagstukken, zoals data-veiligheid, privacy en de machtspositie van dataverzamelaars geïntroduceerd binnen deze praktijken. De vraag wie er eigenaar is van de data komt daarbij vaak naar voren, bijvoorbeeld in de discussie of auto-eigenaren ook de door hun auto gegenereerde gegevens moeten bezitten (Timmer et al. 2014). Of: wie de biologische en fysiologische data bezit die door apps en wearables worden verzameld. En in de landbouwsector gaat het om de vraag of de boer straks nog eigenaar is van de data over zijn eigen land (Munnichs & Bos 2016). Deze vraag leidde in Frankrijk tot een amendement op een wetsvoorstel om data die door internationale technologieleveranciers wordt verzameld toegankelijk te houden voor Franse boeren.<sup>119</sup> Met betrekking tot digitale platformen onderstreept het instituut het belang van data-portabiliteit, zodat consumenten in staat zijn hun opgebouwde gegevens mee te nemen naar een andere aanbieder en de vorming van marktmonopolies wordt tegengegaan (Kreijveld et al. 2014).

Om zicht te houden op datastromen en analyses is transparantie nodig. Als het gaat over gezondheid, is het voor patiënten en consumenten de vraag wat technologieleveranciers en achterliggende derde partijen verzamelen en waarom. En hoe profielen worden gebruikt om tot welke conclusies te komen over gezondheid en gezondheidsrisico's (Geesink et al. 2016). Ook wanneer het gaat over verzekeraars is deze transparantie en uitlegbaarheid van automatische beslissingen een belangrijke aanbeveling (Timmer et al. 2015).

Robotica en artificiële intelligentie (AI) roepen tal van maatschappelijke en ethische vragen op, bijvoorbeeld rond menselijke waardigheid (Royakkers et al. 2012; Van Est & Kool 2015; Royakkers & Van Est 2016). In 2012 riep het Rathenau Instituut het kabinet op een integrale beleidsvisie te ontwikkelen om robotica-ontwikkelingen in de gewenste richting te sturen (Messer 2012). De Nederlandse regering zou tevens moeten streven naar een internationaal verbod op autonome bewapende robots, omdat beslissen over leven en dood niet aan machines overgelaten dient te worden. Om de verkeersveiligheid drastisch te verbeteren, zou de Regering de verplichte invoer van de automatische snelheidsbegrenzers serieus dienen te overwegen. Daarnaast zou de politiek snel aandacht moeten besteden aan de gevolgen van slimme robottechnologieën in de leefomgeving: welke taken willen we wel of juist niet door robots laten verrichten? Welke nieuwe vaardigheden vereist dit van verzorgers en patiënten en wat betekent dit voor privacy- en aansprakelijkheidskwesties? Op het terrein van de arbeid is het van belang dat nieuwe technologie de mens niet reduceert tot een radertje in het systeem, maar arbeid juist verrijkt. Een inclusieve robotsamenleving vraagt om complementaire inzet van mensen en robotica.

---

<sup>119</sup> Project de Loi République numérique. Amendement na artikel 40 A. Zie voor meer informatie [republique-numerique.fr/pages/digital-republic-bill-rationale](http://republique-numerique.fr/pages/digital-republic-bill-rationale)

In de publicatie *Intieme technologie* (Van Est 2014) komen inzichten uit verschillende studies samen. Volgens het Rathenau Instituut versmelten mens en technologie zo snel dat er sprake is van een intiem-technologische revolutie. Het Rathenau Instituut pleit voor een rijksbrede aanpak waarin wordt gekeken naar hoe digitalisering raakt aan fundamentele waarden zoals autonomie, menselijke waardigheid en privacy (Van Est & Rerimassie 2014). Daarnaast pleit het Rathenau Instituut voor een staatscommissie die kijkt naar de betekenis van de intiem-technologische revolutie voor de grondrechten. Tot slot moet mediawijsheid en technologisch burgerschap worden gestimuleerd, zodat burgers mee kunnen praten over de wijze waarop technologie invloed heeft op hun leefomgeving en lichaam.

Bij het ontwikkelen van kaders om de snelle ICT-revolutie maatschappelijk in te bedden kan voortgebouwd worden op ervaringen met de omgang met ethische kwesties rond biomedische technologie. Die ervaring komt van pas omdat ICT steeds meer verweven raakt met de levens- en gedragswetenschappen, waardoor allerlei biomedische technieken in het publieke domein worden toegepast. Aangezien het Biogeneeskundeoverdrag uit 1997 (het Verdrag van Oviedo) een prima basis kan bieden om de menselijke waardigheid ook bij de toepassing van (medische) technologie in het publieke domein te beschermen, raadt het Rathenau Instituut de regering aan dit verdrag te ratificeren. De trend dat ethische discussies die traditioneel met name binnen het biomedische domein werden gevoerd door nieuwe technologie ook steeds meer verschuiven naar technologische praktijken in het dagelijks leven staat ook centraal in het rapport *From Bio to NBIC Convergence* (Van Est et al. 2014), dat is geschreven in opdracht van de Committee on Bioethics van de Raad van Europa.

### **Andere adviesraden en instituten**

Naast de hierboven beschreven adviesraden en instituten komt de thematiek van digitalisering en ethiek ook bij andere adviesorganisaties meer terug. Zo kijkt het Centraal Planbureau in de publicatie *Kiezen voor privacy* naar de markt voor persoonsgegevens. Een effectieve markt voor persoonsgegevens stimuleert innovatie met gebruik van data en geeft mensen de mogelijkheid om te bepalen waar en wanneer ze bereid zijn hun privacy op te geven (CPB 2014). De Onderwijsraad geeft in haar meerjarenagenda ook aan de impact van digitalisering op het onderwijs te gaan bestuderen, waarin ook aandacht is voor de gevolgen voor de privacy en identiteitsontwikkeling van leerlingen, en de machtsverhoudingen tussen onderwijsinstellingen en bedrijven die online leerplatformen beheren (Onderwijsraad 2015: 30).

### **Internationale ontwikkelingen**

#### *European Group on Ethics in Science and New Technologies*

Op Europees niveau speelt de European Group on Ethics in Science and New Technologies (EGE) een belangrijke signalerende rol in discussies over de ethische aspecten van nieuwe technologie. De EGE is een onafhankelijk adviesorgaan van de President van de Europese Commissie en tevens de centrale spil in het netwerk van nationale ethiekraden uit verschillende EU-landen.<sup>120</sup> Sinds de oprichting in 1991 heeft de EGE verschillende opinies uitgebracht waarvan het grootste deel gaat over het biomedische domein. In de laatste jaren heeft de EGE echter ook meer aandacht

---

<sup>120</sup> [ec.europa.eu/research/ege/index.cfm](http://ec.europa.eu/research/ege/index.cfm)



voor digitalisering in haar opinies over informatietechnologie (Salvi 2012) en security en surveillance (Dratwa 2014).

De opinie *Ethics of Information and Communication Technologies* (Salvi 2012) werd door EU-voorzitter Barroso aangevraagd om als referentiepunt te dienen voor een verantwoorde implementatie van de Europese Digitale Agenda (Salvi 2012: 59). Een belangrijk punt is inclusieve toegankelijkheid van ICT, met name voor kwetsbare groepen, zoals minderheden, ouderen en mensen met een beperking. De EGE pleit voor een recht op toegang tot het internet en educatie om te zorgen dat mensen ook de digitale vaardigheden hebben om mee te doen. Daarnaast dienen ook de vrijheid van meningsuiting op het internet en netneutraliteit beschermd te worden. Een ander belangrijk onderwerp is de vrije identiteitsontwikkeling in het digitale tijdperk. Daarbij zijn sociale vaardigheden van belang, waardoor mensen bijvoorbeeld op een verantwoorde manier leren omgaan met sociale media en het internet. Tot slot stelt de EGE dat de mensen ICT-innovaties moeten kunnen omhelzen, zonder daar hun persoonlijke privacy of autonomie voor in te hoeven leveren.

In de opinie *Ethics of Security and Surveillance Technologies* (Dratwa 2014) stelt de EGE dat de verantwoordelijkheid van de staat om veiligheid te garanderen, breder moet worden gezien dan het beschermen van lichamelijke integriteit. Het gaat ook om maatschappelijke en menselijke veiligheid, die mens en maatschappij in staat stelt om zich te ontwikkelen vanuit vrijheid, waardigheid, autonomie en rechtvaardigheid. Fundamentele waarden zoals menselijke waardigheid kunnen niet simpelweg worden uitgeruild tegen veiligheid. Proportionaliteit is het sleutelwoord bij de inzet van veiligheidstechnologie, en daarbij moet ook worden gekeken naar bewezen effectiviteit. De EGE waarschuwt dat profilering kan leiden tot discriminatie, en stelt dat (ethische) aannames die ten grondslag liggen aan algoritmen expliciet moeten worden gemaakt om stigmatisering (*stigmatization by design*) te voorkomen. Dit vereist een onafhankelijke toezichthouder met adequate technische kennis op het niveau van de lidstaten, die ook het aanspreekpunt kan zijn voor burgers die zich onrecht voelen aangedaan, en die ook de maatschappelijke discussie over voor- en nadelen van surveillance aanjaagt.

**Tabel 3** Activiteiten binnen het politiek-bestuurlijk domein op het gebied van agendavorming

Wie/wat	Technologie	Issue	Advies/actie
<i>Wetenschappelijke Raad voor het Regeringsbeleid</i>			
iOverheid	Digitaliserende overheid	privacy, transparantie, autonomie, controle	Besef van transformerende impact van ICT op overheid. Instellen iAutoriteit en iPlatform voor weerbaarheid van burgers
Publieke kern van het Internet	Internet-infrastructuur	veiligheid, censuur, vrije toegang	Publieke kern van het internet vastleggen in internationale verdragen
Robot de Baas	Robotica	werk, inclusie, gelijkheid, autonomie	Inzetten op complementaire samenwerking mensen en robotica
Big data in een vrije & veilige	Big data en algoritmen	privacy, veiligheid, autonomie, discriminatie,	Sterkere focus op het gebruik van gegevens, toezicht op algoritmen,

samenleving		recht op eerlijk proces	nieuwe taken voor toezichhouders
<i>Adviesraad internationale vraagstukken</i>			
Het internet	Internet infrastructuur	Internetvrijheid, privacy, surveillance, informatieveiligheid	Beschermen internetvrijheid. Interdepartementale coördinatie en visie op internetbeleid.
Autonome wapensystemen	Autonome wapensystemen	controle over technologie, verantwoordelijkheid	Betekenisvolle menselijke controle bij inzet autonome wapensystemen
<i>Raad voor de leefomgeving en infrastructuur</i>			
Technologische innovaties in de leefomgeving	Digitalisering (AI, data-infrastructuur, drones, robotica, IoT, VR)	privacy, transparantie, veiligheid, toegang, controle op algoritmen, autonomie	Data-ontwikkeling vraagt kabinetsbrede visie en maatschappelijke debatten over impact op fundamentele waarden
<i>Rathenau Instituut (selectie van publicaties)</i>			
Just Ordinary Robots	Robotica, AI	privacy, autonomie, menselijke waardigheid, controle over technologie	Beleidsvisie op taken over kunnen worden gedragen aan robots, beslissen over leven of dood niet automatiseren.
Werken aan de Robotsamenleving	Robotica, AI, platformen	werkeloosheid, menselijke waardigheid, inclusiviteit	Scholing, inclusieve innovatie, waarborgen tegen monopolisering en uitbuiting digitale platformen
De datagedreven samenleving	Big data, algoritmen	privacy, transparantie, controle op algoritmen, autonomie, discriminatie, machtsverhoudingen	Controle op algoritmen, bescherming van autonomie en gelijkheid. Data zijn niet neutraal: stimuleren van data-geletterdheid
Eerlijk advies	Health apps, wearables, persuasieve technologie	privacy, autonomie, betrouwbaarheid van technologie, transparantie, machtsverhoudingen	Beschermen privacy en autonomie, keurmerk voor betrouwbare e-coaches, verplichte bewijslast voor overheidsinzet gedragsbeïnvloeding
Intieme technologie	Digitalisering breed	privacy, autonomie, menselijke waardigheid	Rijksbrede aanpak op de impact van digitalisering op grondrechten, bevorder technologisch burgerschap
<i>European Group on Ethics in Science and New Technologies</i>			
Ethics of Information and Communication Technologies	Digitalisering breed	privacy, menselijke waardigheid, autonomie, vrijheid van meningsuiting, toegang tot technologie	Toegang tot ICT. Stimuleren digitale vaardigheden, vrije online identiteitsontwikkeling en verantwoord persoonlijk gebruik van ICT
Ethics of Security and Surveillance Technologies	Big data, surveillance-veiligheidstechnologie	veiligheid, privacy, menselijke waardigheid, autonomie, discriminatie	Verplicht expliciet maken assumpties van algoritmen. Menselijke waardigheid niet uitruilen voor andere waarden zoals veiligheid

In de fase van beleidsvorming en -bepaling vindt de vertaling van de beleidsvoorbereidende rapporten en adviezen naar visies, beleid, regelgeving en wetten plaats. We kijken hier naar de actoren die institutioneel belast zijn met het bepalen van het beleid en het vormgeven aan wet- en regelgeving: het kabinet en de ministeries en het parlement bestaande uit de Eerste en de Tweede Kamer. We beschrijven de acties die worden ondernomen om met ethische en maatschappelijke vragen van digitalisering om te gaan. Zoals aan het begin van de analyse aangegeven, beschrijven we de actoren aan de hand van hun rol in het institutionele landschap, maar de acties die de actoren ondernemen kunnen ook meer in het domein van beleidsagendering liggen, denk aan een ministerie dat onderzoek uitzet of een expertgroep instelt om de beleidsvorming te ondersteunen.

### **Ministerie van Economische Zaken**

In het beleid van het Ministerie van Economische Zaken is er diverse malen aandacht geweest voor de ethische aspecten van digitalisering. In de visie op telecommunicatie, media en internet (Kamerstukken II 2013-2014, 26643 nr.300) wordt het belang van een vrij en open internet en digitale keuzevrijheid benadrukt, zowel ter bescherming van burgerlijke vrijheden als ten behoeve van de (vrije) markt. In lijn hiermee is er aandacht voor digitale platformen (Kamerstukken II 2013-2014, 26643 nr.345) en hun (machts)positie als toegangspoort tot informatie en diensten. Gekeken wordt of er maatregelen nodig zijn om vrije keuze en concurrentie te stimuleren. In de brief over toekomstbestendige regelgeving wordt hier verder op in gegaan, nieuwe generieke wetgeving is vooralsnog niet wenselijk en er wordt gestreefd om meer ruimte te creëren voor innovaties zoals platformen en de deeleconomie. Daarbij is het echter wel van belang om oog te houden voor het beschermen van publieke waarden (Kamerstukken II 2014-2015, 33009, nr.10 & 12).

Privacy heeft een plek in de *visie telecommunicatie*.<sup>121</sup> In de brief over big data en profilering wordt verder op dit thema ingegaan (Kamerstukken II 2014-2015, 32761, nr.76). De brief beschrijft dat big data en profilering kunnen zorgen voor een inbreuk op het recht op privacy en het recht op gelijke behandeling. Het wettelijk kader, dat bestaat uit de Wet bescherming persoonsgegevens (Wbp), de Telecommunicatiewet en de Algemene wet gelijke behandeling (Awgb), biedt hier bescherming. Toezicht op de naleving van deze drie wetten gebeurt respectievelijk door de Autoriteit Persoonsgegevens, de Autoriteit Consument en Markt en het College voor de Rechten van de Mens. Tegelijkertijd geeft de brief aan dat een puur juridische benadering niet zal volstaan; transparantie en vertrouwen zijn ook nodig. Er wordt aangekondigd dat een high level expertgroep over big data wordt opgericht, die in 2016 een advies zal opleveren over de relatie tussen big data en bescherming van grondrechten als privacy en gelijke behandeling.

Het meest direct is het onderwerp ethiek recent aan de orde geweest naar aanleiding van de motie Ester c.s. (Kamerstukken I, 2013-2014, 33750 XIII) waarin de regering wordt verzocht 'structureel plaats in te ruimen in het technologie- en innovatiebeleid voor reflectie op ethische vragen'. In reactie op de motie Ester komt minister Kamp in juni 2016 met de brief *Ethische aspecten van het innovatiebeleid* (Kamerstukken I, 2015-2016, 33009, nr. 16). De brief stelt dat snelle technologische

---

<sup>121</sup> In de *visie telecommunicatie* wordt ook gesproken over het uitbreiden van de in de Telecommunicatiewet vastgelegde zorgplicht van bedrijven om op het gebied van integriteit, continuïteit en bescherming van de persoonlijke levenssfeer passende maatregelen te nemen. In de voortgangsrapportage (Kamerstukken II 2013-2014, 26643 nr. 345) wordt echter de conclusie getrokken dat deze zorgplicht niet wordt aangepast, onder andere omdat de generieke zorgplicht in de Wbp afdoende wordt geacht.

ontwikkelingen zorgen voor ethische kwesties zoals vragen over versmelting tussen mens, technologie en natuur en vragen over de impact op fundamentele waarden zoals privacy en autonomie. De brief beschrijft vervolgens de huidige initiatieven die vanuit het ministerie worden ontplooid op het gebied van ethiek en zegt toe deze rapportage onderdeel te maken van de jaarlijkse Voortgangsrapportage Bedrijvenbeleid. Ethiek krijgt in het innovatiebeleid aandacht binnen het onderzoek, via het NWO-programma Maatschappelijk Verantwoord Innoveren (MVI) en het sociaal innovatieprogramma Topsector Energie (STEM). Op het gebied van big data wordt verwezen naar de high level expertgroep over big data, die is aangekondigd in de brief over big data en profilering. Tot slot benoemt de brief ook dat er binnen de afdelingen van het ministerie die zich bezighouden met landbouw, voedsel en veehouderij<sup>122</sup> een handreiking is over Ethiek in Beleid. Deze ondersteunt beleidsmakers in de omgang met ethische aspecten in de beleidsontwikkeling.<sup>123</sup>

Hoewel er binnen afdelingen verschillende initiatieven lopen op het gebied van ethiek en (digitale) innovatie, is er geen overkoepelende visie of coördinatie op het thema. Zo is er een handleiding over de omgang met ethische aspecten in beleidsontwikkeling voor de domeinen van voedsel, agro en veehouderij, maar niet voor andere beleidsterreinen. De expertgroep over big data – waarvan de resultaten nog moeten worden gepubliceerd – toont dat er aandacht is voor de ethische aspecten omtrent big data, maar dat deze zich nog bevindt in een beleidsvoorbereidende, adviserende fase. Andere technologische ontwikkelingen die onderdeel zijn van digitalisering worden nog niet opgepakt. De vraag om structurele monitoring van ethische aspecten van het innovatiebeleid en de aanvullende vraag van de vaste Kamercommissie EZ (Kamerstukken I, 2015-2016, 33009, nr. D) om ook beleidsconsequenties aan de monitoring te verbinden, kan betekenen dat de aandacht daarvoor de komende jaren wordt uitgebouwd.

### **Ministerie van Veiligheid en Justitie**

Het thema veiligheid en bescherming van persoonlijke levenssfeer zijn belangrijke onderwerpen voor het Ministerie van Veiligheid en Justitie. In 2007 werd de Adviescommissie 'Veiligheid en persoonlijke levenssfeer' (Commissie Brouwer-Korf) gevraagd om te adviseren over de invloed van technologische ontwikkelingen op de bescherming van veiligheid en de persoonlijke levenssfeer. Op basis van het advies van de commissie Brouwer-Korf en de evaluatie van de Wet bescherming persoonsgegevens wordt voorgenomen om een meldplicht voor datalekken in te voeren en de boetebevoegdheid van de toezichthouder (thans de Autoriteit Persoonsgegevens) uit te breiden (Kamerstukken II 2009-2010 31051, nr.5).

De discussie over veiligheid en privacy komt terug in de notitie *Privacybeleid* (Kamerstukken II, 2010-2011, 32761, nr.1) en de latere notitie *Vrijheid en veiligheid in een digitale samenleving* (Kamerstukken II, 2013-2014, 26643, nr.298). Hierin worden maatregelen aangekondigd als bewustwordingscampagnes gericht op digitale weerbaarheid, het stimuleren van privacy en security by design in aanbestedingstrajecten, en de verplichte privacy impact assessment (PIA) voor de

---

<sup>122</sup> Afdelingen van het voormalige Ministerie van Landbouw, Natuur en Voedselkwaliteit

<sup>123</sup> De handleiding wordt op aanvraag van de vaste commissie Economische Zaken ook naar de Kamer gestuurd (Kamerstukken II, 2015-2016, 33009 nr. D).

ontwikkeling van nieuwe wetgeving en beleid. Het thema is echter zo complex dat bepaalde zaken verder doordacht moeten worden. Dat uit zich in de aanvraag in 2014 van het WRR advies over de rol van big data in het veiligheidsdomein. (Het WRR-advies is in april 2016 verschenen.) Een van de vragen is of het nodig is om een onderscheid te maken tussen toegang tot gegevens en het gebruik van deze gegevens.

Op het gebied van cyberveiligheid is de Nationale Cybersecurity Strategie (NCSS) geformuleerd. De NCSS beoogt een integrale aanpak van cybersecurity vanuit publiek-private samenwerking (Kamerstukken II 2013-2014, 26643, nr. 291). Als onderdeel van de strategie is het Nationale Cyber Security Centrum (NCSC) opgericht dat reageert op incidenten en dreigingen en werkt aan het versterken van digitale weerbaarheid en veiligheid. Het kabinet komt op verzoek van de Kamer ook met een kabinetsstandpunt over encryptie (Kamerstukken II, 2015-2016, 26643, nr. 383). Daarin geeft het kabinet aan dat ze het instellen van wettelijke beperkingen op encryptie om inlichtingen- en veiligheidsdiensten toegang tot gegevens te verschaffen – zoals de FBI die toegang wilde tot de versleutelde iPhone van een verdachte – niet wenselijk acht.

Tegelijk kijkt het kabinet naar de mogelijkheden van digitale technologie in het veiligheidsdomein. Het wetsvoorstel computercriminaliteit III en conceptwetsvoorstel Wet op de inlichtingen en veiligheidsdiensten (Wiv) – waarin het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties de leidende rol heeft – voorzien in nieuwe bevoegdheden voor de overheid. Beide voorstellen ontvangen stevige kritiek:<sup>124</sup> de overheid zou te vergaande bevoegdheden krijgen tot ongerichte informatieverzameling die een inbreuk zijn op de persoonlijke levenssfeer. Het voorstel voor de Wiv ligt nu ter advisering bij de Raad van State.

De discussie op het beleidsterrein van Veiligheid en Justitie richt zich dus op de thema's privacy en veiligheid, waarin wordt getracht deze niet als tegenover elkaar staande waarden te zien, maar in elkaars verlengde te plaatsen (Kamerstukken II 2013-2014, 32761, nr. 83). Op verschillende momenten reageert de minister van Veiligheid en Justitie op vragen vanuit het parlement om te komen tot een visie op privacy en de bescherming van de persoonlijke levenssfeer. De vraag is een van de aanleidingen voor de notitie Privacybeleid, en wordt later onder andere door Kamerleden Thieme en Oosenbrug opnieuw naar voren gebracht.<sup>125</sup> In reactie op de vraag van lid Oosenbrug stelt minister Van der Steur dat de visie in verschillende onderdelen terug te zien is in de brieven over *Vrijheid en veiligheid in de digitale samenleving, E-privacy en big data en profileren*.<sup>126</sup> Een alomvattende visie zou volgens de minister zo abstract zijn dat zij geen recht kan doen aan de verschillende perspectieven en invalshoeken op deelterreinen. Iedere minister is daardoor verantwoordelijk voor de privacyaspecten die met diens beleidsterrein zijn verbonden. Privacy wordt hier voornamelijk benaderd vanuit het perspectief van gegevensverzameling en gegevensbescherming.

---

<sup>124</sup> Kritiek op het wetsvoorstel computercriminaliteit III werd geuit tijdens een hoorzitting over het wetsvoorstel in de Tweede Kamer (zie [tweedekamer.nl/vergaderingen/commissievergaderingen/details?id=2016A00399](http://tweedekamer.nl/vergaderingen/commissievergaderingen/details?id=2016A00399)) Kritiek op het conceptwetsvoorstel Wiv werd onder andere door het College voor de Rechten van de Mens, Bits of Freedom & VNO-NCW tijdens de internetconsultatie naar voren gebracht (zie [internetconsultatie.nl/wiv/reacties](http://internetconsultatie.nl/wiv/reacties))

<sup>125</sup> Respectievelijk Kamerstukken II, 2010-2011, 32761, nr.1; Kamerstukken II 2013-2014, 32761, nr. 83; Kamerstukken II 2013-2014, 32761, nr. 89

<sup>126</sup> Respectievelijk Kamerstukken II, 2013-2014, 26643, nr.298; Kamerstukken II 2014-2015, 32761, nr. 49; Kamerstukken II 2014-2015, 32761, nr.76

### **Ministerie van Onderwijs, Cultuur en Wetenschap**

De acties die het Ministerie van Onderwijs, Cultuur en Wetenschap neemt om met de maatschappelijke impact van digitalisering om te gaan liggen met name op het gebied van digitale vaardigheden. Met het platform Onderwijs 2032 wordt nagedacht over de toekomst van het onderwijs. Digitalisering en robotisering zorgen ervoor dat de banen van de toekomst er anders uit zullen zien, en het onderwijs moet leerlingen voorbereiden op deze snel veranderende digitale wereld.<sup>127</sup> Digitale geletterdheid moet onderdeel worden van het kerncurriculum van het onderwijs, waarbij het gaat om kennis van ICT, computational thinking, en mediawijsheid – het aanleren van normen en waarden als het gaat om privacy, veiligheid, online omgangsvormen, reputatie en beeldvorming (Kamerstukken II, 2015-2016, 31293, nr.278). Daarnaast zet het kabinet in op continue scholing – ‘een leven lang leren’ – als strategie om met veranderende eisen op de arbeidsmarkt om te gaan (Kamerstukken II 2015-2016, 30012, nr. 55).

Op het gebied van wetenschappelijk onderzoek wordt gestimuleerd om vroegtijdig over de maatschappelijke impact van nieuwe innovaties na te denken vanuit het concept van *maatschappelijk verantwoord innoveren*. In de wetenschapsvisie wordt het belang van vroegtijdig debat over de maatschappelijke implicaties van wetenschap en technologie onderstreept. Door gebruikers en belanghebbenden intensief te betrekken in het onderzoek kan het beter bijdragen aan het oplossen van maatschappelijke vraagstukken. Een voorbeeld dat daarbij wordt genoemd, is het onderzoeksproject ‘Digitaal huisrecht 2.0’ naar de bescherming van de persoonlijke levenssfeer in de digitaliserende wereld (Kamerstukken II, 2014-2015, 29338, nr.141). Waar het gaat over het gebruik van big data in het onderzoek en het onderwijs moeten ethische vragen in een vroegtijdig stadium worden besproken, en bij elke stap van de ontwikkeling geëvalueerd (Kamerstukken II 2015-2016, 31288, nr. 545).

### **Ministerie van Sociale Zaken en Werkgelegenheid**

Op 29 september 2014 noemt minister Asscher van Sociale Zaken en Werkgelegenheid (SZW) in een speech op het SZW-jaarcongres de opkomst van robotisering als een mogelijke bedreiging voor de werkgelegenheid. In reactie op de motie van Kamerlid Van Ojik (Kamerstukken II 2013-2014, 27406, nr. 212) komt de minister met een brief waarin de effecten van automatisering op de arbeidsmarkt worden besproken. Het onderwerp is omgeven door onzekerheid, maar om te kunnen anticiperen op verschillende ontwikkelingen is het noodzakelijk dat beleidsmakers hier aandacht aan besteden. Het CPB en de SER worden verzocht onderzoek te doen naar de relatie tussen technologie en werkgelegenheid, en ook het Rathenau Instituut (op verzoek van de Tweede Kamer) en de WRR (2015) brengen studies uit over dit onderwerp.

Robotisering heeft de potentie om menselijke waardigheid te ondersteunen door zwaar werk over te nemen en werk ‘veiliger, minder belastend en leuker’ te maken (WRR 2015: 3), maar tegelijkertijd kunnen er ook werkloosheid (voor bepaalde groepen mensen) en toenemende maatschappelijke ongelijkheid ontstaan. In de reactie op het Rathenau-rapport *Werken aan de robotsamenleving* (Van Est & Kool 2015) geeft het ministerie aan dat ingezet wordt op goede opleiding en soepele

---

<sup>127</sup> Hierbij verwijst de minister naar het WRR-advies *De robot de baas*.

transitie naar nieuw werk. Dit komt ook terug in het leven-lang-leren-beleid van het ministerie van OCW (Kamerstukken II 215-2016, 30012, nr. 55). In de adviesaanvraag aan de SER over de effecten van robotisering, automatisering en digitalisering op de arbeidsmarkt en -verhoudingen wordt ook aandacht gevraagd voor de flexibilisering van arbeid, en hoe de positie van werknemers van digitale platformen gewaarborgd kan worden, met het oog op gezond en veilig werken. Naar aanleiding van het SER-advies zal het kabinet met een brede inclusieve agenda komen op het thema robotisering en arbeid (Kamerstukken II 2015-2016, 29544, nr. 725).

### **Ministerie van Buitenlandse Zaken**

Zoals hiervoor beschreven roepen de WRR en Adviesraad Internationale Vraagstukken (AIV) op tot een geïntegreerd internationaal internetbeleid. Met de kabinetsreactie op de rapporten van de AIV en de WRR geeft het kabinet gehoor aan deze oproep namens de ministers van Buitenlandse Zaken, Economische Zaken, Defensie, Binnenlandse Zaken en Koninkrijksrelaties, en Veiligheid en Justitie (Kamerstukken II, 2015-2016, 26643, nr.411). Het kabinet onderschrijft het belang van een interdepartementaal gecoördineerde visie en zegt toe een dergelijke visie te gaan ontwikkelen vanuit het belang van een vrij, open en veilig internet. Fundamentele rechten zijn volgens het kabinet online evenzo van toepassing als offline. In de mensenrechtenrapportage 2015 (Kamerstukken II, 2015-2016, 32735 nr. 154) wordt dit perspectief onderschreven. Nederland brengt het onderwerp in april 2016 onder de aandacht door, als organisator, het thema 'digitale rechten' een centrale plek te geven tijdens de Global Conference on Cyberspace en aandacht te vragen voor de ethiek van algoritmen. Deze acties zijn in lijn met de adviezen van de WRR en AIV om mensenrechten het speerpunt te maken in het internationale internetbeleid.

Met betrekking tot de bescherming van mensenrechten concludeert de minister in de brief over zorgplichten van bedrijven op het gebied van internationaal maatschappelijk verantwoord ondernemen (IMVO)<sup>128</sup> dat er procedurele drempels zijn in het aansprakelijk stellen van bedrijven, zoals hoge kosten en beperkte mogelijkheden tot collectieve acties (Kamerstukken II, 2015-2016, 26485, nr. 219). Het kabinet doet daarom onderzoek naar de wenselijkheid van een wetswijziging die het mogelijk maakt om onder bepaalde omstandigheden ook collectieve vorderingen tot schadevergoeding in te stellen. Deze collectieve acties zouden als het gaat om het doen van een beroep op het recht op bescherming van de persoonlijke levenssfeer relevant kunnen zijn.

Tot slot brachten de Ministeries van Buitenlandse Zaken en Defensie een brief uit over autonome wapensystemen, als reactie op het advies van de AIV (2015) dat autonome wapensystemen alleen kunnen worden ingezet mits er sprake is van betekenisvolle menselijke controle (Kamerstukken II, 2015-2016, 34300 X, nr. 88). Er moet daarom al in de ontwerpfase van wapensystemen worden gedacht over de toewijzing van verantwoordelijkheid en aansprakelijkheid, en bij het aanschaffen van systemen dient de Adviescommissie Internationaal Recht en Conventioneel Wapengebruik op betekenisvolle controle te toetsen. In de brief wordt gesteld dat ethische vraagstukken over menselijke waardigheid bij autonome wapensystemen niet anders liggen dan bij conventionele wapensystemen als betekenisvolle controle is voorzien. Het kabinet wijst de mogelijke ontwikkeling

---

<sup>128</sup> Zoals vastgelegd in de OESO-richtlijnen voor multinationale ondernemingen en de United Nations Guiding Principles on Business and Human Rights (UNGP's)

en inzet van volledig autonome wapens – waarbij menselijke controle niet meer mogelijk is – op voorhand af. Een moratorium acht het kabinet net als de AIV niet haalbaar, hoewel NGO's en wetenschappers hier wel voor pleiten. Bijvoorbeeld in de brief tegen autonome wapens waar in het begin van deze studie naar werd verwezen, die door Stephen Hawking, Elon Musk en 1000 andere experts werd ondertekend (Future of Life Institute 2015).

### **Ministerie van Binnenlandse Zaken en Koninkrijksrelaties**

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties houdt zich op verschillende manieren met digitalisering bezig. Het kijkt naar digitalisering van de overheidsdienstverlening, maar is ook het verantwoordelijke ministerie als het gaat om de impact van digitalisering op de grondrechten. Op dit moment loopt er naar aanleiding van het advies van de Staatcommissie Thomassen een herziening van artikel 13 van de Grondwet, zoals hierboven is besproken (Kamerstukken II 2010-2011, 31570, nr. 20).

Met betrekking tot de digitalisering van de overheid onderschrijft de minister van BZK in reactie op het rapport iOverheid van de WRR in 2011 dat digitalisering niet alleen een instrumentele verandering betreft, maar de organisatie en de taken van de overheid zelf fundamenteel verandert. Dat besef moet verankerd worden in het werk van de overheid (Kamerstukken II, 2011–2012, 26 643, nr. 211). De aanbeveling van de WRR tot het oprichten van een iAutoriteit die burgers bijstaat bij problemen met de digitale overheid wordt niet overgenomen, omdat die verantwoordelijkheden onderdeel van de gehele overheidsdienstverlening zijn. Naar aanleiding van herhaaldelijke problemen bij ICT-projecten bij de overheid initieert de Tweede Kamer in 2012 een parlementair onderzoek, dat wordt georganiseerd door de tijdelijke commissie ICT, ook wel de commissie Elias genoemd. In haar eindrapport uit de commissie sterke kritiek op het overheidsbeleid (Kamerstukken II, 2014-2015, 33326, nr. 5). In reactie op het rapport wordt de toetsing en controle op ICT-projecten versterkt, onder meer door het instellen van een Bureau ICT Toetsing (Kamerstukken II, 33326, nr. 13). De controle en toetsing richt zich hier echter vooral op de technische en bestuurlijke dimensie en niet zozeer op de maatschappelijke en ethische impact van overheids-ICT.

Tot slot loopt er op dit moment een herziening van de Wet op de inlichtingen en veiligheidsdiensten (Wiv) uit 2002. Een belangrijke aanleiding vormt de techniek-afhankelijke formulering van de interceptiebepalingen in de Wiv. Het onderscheid dat daarin wordt gemaakt tussen kabelgebonden communicatie en de ether valt niet meer te rijmen met de ontwikkeling van communicatiemiddelen en dataverkeer (Kamerstukken II 2014-2015, 33820 nr. 4). Het wetsvoorstel werd via een internetconsultatie aan experts en maatschappelijke organisaties voorgelegd, en er werd ook een privacy impact assessment gemaakt door het Privacy & Identity Lab (Kamerstukken II 2015-2016, 33820 nr. 8) Het voorstel ontving scherpe kritiek vanuit de Kamer vanwege de disproportionele impact op privacy die nieuwe bevoegdheden met zich mee zouden brengen en het gebrek aan adequate waarborgen. Een aangepast voorstel ligt nu ter advisering bij de Raad van State.

### **Parlement**

De Eerste en de Tweede Kamer spelen als volksvertegenwoordiging een belangrijke rol bij het genereren van aandacht voor maatschappelijke en ethische vragen omtrent digitalisering. En vanuit hun controlerende taak volgen ze kritisch het regeringsbeleid. Vragen vanuit de Kamer spelen een belangrijke rol in de visies en brieven van het kabinet waarin wordt gegaan op het beleid omtrent



technologische ontwikkelingen. De ePrivacy-brief van het ministerie van EZ reageert op de moties van Verhoeven en Gesthuizen (Kamerstukken II, 2011-2012, 24 095, nr. 294) en Recourt c.s. (Kamerstukken 2011-2012, 32761, nrs. 10 en 11). Naar aanleiding van de ePrivacy-brief vraagt de Kamer om meer informatie over big data en profilering, waaruit een volgende Kamerbrief volgt en een *high level expert group* wordt ingesteld om de impact van big data op fundamentele rechten te onderzoeken (Kamerstukken II 2014-2015, 32761, nr. 76). Zoals hiervoor aangegeven, wordt ook de minister van Veiligheid en Justitie verschillende malen gevraagd om een visie op digitale privacy en veiligheid te ontwikkelen. Zoals gezien speelt bij de agendering van vraagstukken ook maatschappelijke actoren, adviesraden en onderzoeksinstituten een rol. De Big Brother Award van Bits of Freedom vormt bijvoorbeeld de aanleiding voor Kamervragen van de leden Verhoeven en Schouw, waarop wordt gereageerd met de nota *Vrijheid en veiligheid in de digitale samenleving* (Kamerstukken II, 2013-2014, 26643, nr. 298).

Op het gebied van privacy en veiligheid vraagt het parlement de regering dus herhaaldelijk om een visie te vormen. Op andere aspecten van digitalisering zijn vragen vaak meer gedreven door actuele gebeurtenissen. Berichten die in de media spelen vormen de aanleiding voor Kamervragen over de wenselijkheid van bepaalde technologische ontwikkelingen, bijvoorbeeld over het verzamelen van gegevens uit de auto door autofabrikanten, initiatieven van banken die gebruik willen maken van big data, het ontduiken van regulering door Uber, controle en transparantie van zelfhandelende algoritmen op de beurs, of senioren die de digitalisering van de overheid te snel vinden gaan.<sup>129</sup>

Met de motie Gerkens c.s. en de motie Ester c.s. wordt expliciet aandacht gevraagd voor de ethische aspecten die samenhangen met respectievelijk digitalisering en NBIC convergentie. In deze moties zien we, zoals in hoofdstuk 4 beschreven, de historisch terugkerende vraag of het politiek-bestuurlijke stelsel adequaat is toegerust om om te gaan met de ethische vragen omtrent nieuwe technologische ontwikkelingen. De vragen getuigen van een behoefte aan structurele reflectie en discussie over de impact van technologische ontwikkelingen. De vraag van Ester c.s. om jaarlijks te rapporteren over de rol van ethiek in het innovatiebeleid dient dan ook begrepen te worden als een initiatief om een structureel terugkerende politiek-ethische discussie over dit onderwerp in de Eerste Kamer mogelijk te maken.<sup>130</sup>

Naast de vragen van Kamerleden wordt er ook op het niveau van politieke partijen nagedacht over technologie. Tweede Kamerlid Lucas presenteerde namens de VVD een robotagenda *Robotisering zonder achterblijvers* (Lucas 2016), waarin wordt gepleit om ruimte te geven voor innovatie en tegelijkertijd in te zetten op educatie zodat mensen mee kunnen bewegen met een veranderende omgeving, en op het gebied van ethiek wordt gepleit voor onderzoek naar de waarde van een Nationale Ethiek Commissie, voor het behouden van een goede balans tussen mens en technologie. D66 geeft haar visie op technologische ontwikkelingen in haar *Techvisie* (Verhoeven et al. 2016). Daarin stelt de partij dat de politiek discussie nu nog te veel wordt gevoerd aan de hand

<sup>129</sup> Respectievelijk Aangangsels Handelingen II 2015–2016, 1488; Aangangsels Handelingen II 2013–2014, 1658; Aangangsels Handelingen II 2013–2014, 1869; Aangangsels Handelingen II 2014–2015, 1818; Aangangsels Handelingen II 2015-2016, 2421.

<sup>130</sup> Gesprek Peter Ester, 14-06-2016

van incidenten. De snel veranderende samenleving heeft een duidelijke toekomstvisie. Volgens D66 zouden technologie en internet een prioriteit van het kabinet moeten zijn en daarbij hoort een minister van Economie, Technologie en Privacy. D66 zet in op inclusieve digitale vaardigheden, digitale keuzevrijheid, goede versleuteling en bescherming van persoonsgegevens, en transparantie over gegevensverzameling en algoritmische beslissingen. Een belangrijke aanbeveling is om de positie van toezichhouders – zoals de ACM (digitale keuzevrijheid), de Autoriteit Persoonsgegevens (privacy), het NCSC (cybersecurity) en de CTIVD (veiligheidsdiensten) – te versterken. Internetreuzen zouden een zorgplicht moeten hebben zoals de banken, vanwege hun nutsfunctie op het gebied van informatie. En bedrijven die slechte software maken moeten daarvoor ook beter aansprakelijk kunnen worden gesteld. De aanbevelingen uit de Techvisie komen terug in het verkiezingsprogramma van de D66. Daarin wordt ook een iPlatform voor kritische reflectie op de digitale samenleving voorgesteld en een speciale commissie die een jaarlijkse bespreking van de relatie tussen technologie en grondrechten in de Kamer faciliteert (D66 2016).

### **Internationale ontwikkelingen**

#### *EU beleid en regelgeving*

De belangrijkste pijler in het Europese beleid op het gebied van digitalisering is de strategische agenda voor een *Digital Single Market*.<sup>131</sup> In deze agenda staat het economische perspectief centraal, maar wordt tevens gepleit voor een inclusieve en veilige digitale samenleving. Expliciete aandacht voor de ethische vragen is er vanuit het *Onlife Initiative* een werkgroep waarin twaalf internationale experts werden uitgenodigd om te na te denken over hoe digitale technologie ons menszijn verandert. Het resultaat is het *Onlife Manifesto* (EC 2013), een aanzet om nieuwe concepten te ontwikkelen om de fundamentele impact van digitalisering op de mens en zijn sociale omgeving te kunnen begrijpen. Die nieuwe concepten hebben we nodig om na te denken over de vervagende grenzen tussen mens en techniek, het beschermen van onze privéruimte, onze aandacht, zelfbeschikking en autonomie. Het manifest vormt belangrijke input voor vragen over de maatschappelijke en ethische impacts van technologische ontwikkelingen in het onderzoeksprogramma Horizon 2020.

Ook op het niveau van wet- en regelgeving zijn er belangrijke ontwikkelingen op Europees niveau. De Nederlandse wetgeving houdt zich in belangrijke mate aan Europese richtlijnen en verordeningen als het gaat om digitalisering. De meest significante verandering op dit vlak is de vervanging van de Richtlijn gegevensbescherming 95/46/EG door de Algemene Verordening Gegevensbescherming EU 2016/679. Belangrijke veranderingen zijn het verhogen van de boetebevoegdheid van de toezichthouder; het versterken van de rechten van het individu (bijvoorbeeld op het gebied van dataportabiliteit en het verwijderen van zijn gegevens), en het verzwaren van de verplichtingen van de dataverwerkende partij (bijvoorbeeld om *privacy by design* en *privacy by default* toe te passen).<sup>132</sup>

---

<sup>131</sup> COM (2015) 192 final

<sup>132</sup> Bijvoorbeeld door de privacyinstelling op een sociaal netwerk standaard in te stellen op beperkte zichtbaarheid, in plaats van voor iedereen toegankelijk.

Een andere belangrijke ontwikkeling was het ongeldig verklaren van de *Safe-Harbor*-overeenkomst over gegevensuitwisseling tussen Europa en de VS. Met betrekking tot de *Safe-Harbor*-overeenkomst stelde de Europese Commissie dat gegevens van Europese burgers in de VS net zo goed beschermd dienen te zijn als in de Europese Unie, als een wettelijk vereiste voor een makkelijke internationale uitwisseling van gegevens. Naar aanleiding van de onthulling van Snowden spande de Oostenrijker Schrems een rechtszaak aan bij het Europese Hof van Justitie. Omdat de Snowden-onthullingen aantoonde dat gegevens van Europese burgers in de VS niet goed beschermd waren, werd de *Safe-Harbor*-overeenkomst ongeldig verklaard. Een nieuwe overeenkomst over het uitwisselen van gegevens tussen Europa en de VS – de EU-US Privacy Shield – moet voor betere bescherming van persoonlijke gegevens zorgen.<sup>133</sup>

### *Europees Parlement*

De Commissie Juridische Zaken (JURI-commissie) van het Europees Parlement publiceerde op 31 mei 2016 een concept-rapport over robotica en kunstmatige intelligentie (2015/2103(INL)). Om met de ethische uitdagingen van deze ontwikkelingen om te gaan moet een set van fundamentele kernwaarden worden opgesteld. Principes die kunnen worden toegepast in iedere fase in het contact tussen robots, kunstmatige intelligentie en mensen. De JURI-commissie signaleert als aandachtspunten: veiligheid, privacy, integriteit, menselijke waardigheid en autonomie. Daarnaast komen ook andere aspecten aan de orde zoals standaardisatie, intellectueel eigendom, eigendom van data, werkgelegenheid en aansprakelijkheid. De ethische principes heeft de JURI-commissie vastgelegd in een voorstel voor een Handvest over Robotica (*Charter on Robotics*). Dit handvest is opgebouwd bevat een ethische code voor robotbouwers,<sup>134</sup> een code voor commissies betreffende onderzoeksethiek<sup>135</sup> en een model voor gebruikers over toegestane handelingen met robots.<sup>136</sup> De JURI-commissie adviseert dat er een Europees Agentschap opgericht wordt voor robotica en kunstmatige intelligentie zodat deze entiteit aan publieke instellingen op Europees en nationaal niveau kan adviseren over techniek, ethiek en regelgeving.<sup>137</sup>

Het concept-rapport is gericht op de totstandkoming van een resolutie die het Europees Parlement kan aannemen. Het Europees Parlement kan daardoor de Europese Commissie verzoeken het Parlement passende ontwerpen tot vaststelling van nieuwe (of tot wijziging van bestaande) besluiten voor te leggen.<sup>138</sup>

### *Pleidooien voor digitale rechten*

De Labour partij in het Verenigd Koninkrijk laat in 2014 een onderzoek uitvoeren naar een digitale agenda voor het Verenigd Koninkrijk. Op basis van het onderzoek wordt onder andere aanbevolen om sterk in te zetten op digitale vaardigheden om te zorgen dat iedereen kan profiteren van de digitale samenleving. Daarnaast wordt ook opgeroepen om een ethisch raamwerk op te stellen dat

<sup>133</sup> Zie [justitia.nl/privacy/privacy-shield.html](http://justitia.nl/privacy/privacy-shield.html); en [justitia.nl/privacy/safe-harbor.html](http://justitia.nl/privacy/safe-harbor.html)

<sup>134</sup> Code of Ethical Conduct for Robotics Engineers.

<sup>135</sup> Code for Research Ethics Committees.

<sup>136</sup> License for Users.

<sup>137</sup> Punt 8 van het concept-rapport.

<sup>138</sup> Artikel 46 j.o. 52 Reglement van het Europees Parlement.

beleidsmakers moet helpen om te gaan met ethische vragen omtrent digitale ontwikkelingen (*Digital Government Review 2014*). De roep om reflectie en bescherming van fundamentele waarden komt in het Verenigd Koninkrijk ook naar voren in verschillende initiatieven voor een *Digital Bill of Rights*. Berners-Lee, een van de grondleggers van het wereldwijde web, roept in 2014 op om een Magna Carta voor het web op te stellen (Kiss 2014). De Liberale Democraten publiceren in 2015 een oproep om input te verzamelen voor een voorstel voor bescherming van fundamentele rechten op het web.<sup>139</sup> Het *Digital-Liberties*-initiatief leidt een campagne met steun vanuit verschillende politieke partijen om het Britse Parlement aan te zetten om een *Digital Bill of Rights* aan te nemen. Belangrijke principes die worden aangegeven voor het wetsvoorstel zijn: het eigenaarschap van persoonlijke gegevens als recht; gelijke toegang tot het internet voor iedereen; het tegengaan van monopolisering; en het stoppen van massa-surveillance.<sup>140</sup>

Verschillende andere landen werken ook aan wetten waarin internetrechten worden vastgelegd. De Franse regering werkt aan het wetsvoorstel *Republique Numerique*. In 2014 en 2015 werd er een grote internetconsultatie opgezet waarin iedereen kon reageren en bijdragen aan het voorstel. Het wetsvoorstel is inmiddels door de Franse Nationale Vergadering aangenomen en ligt nu ter bespreking en goedkeuring bij de Franse Senaat. In het voorstel staan de volgende elementen centraal: het vrijer beschikbaar maken van open data; het versterken van de rechten van internetgebruikers; en een inclusieve digitale samenleving. Dat uit zich onder andere in een versterking van het recht op dataportabiliteit,<sup>141</sup> het beschermen van netneutraliteit, betere mogelijkheden voor jongeren om gegevens over hun jeugd te laten verwijderen, een recht om aan te geven wat er met persoonlijke gegevens gebeurt na het overlijden, en verplichte transparantie van platformen over hoe ze betaald worden voor bijvoorbeeld de ranking van producten op hun site.<sup>142</sup>

De roep om transparantie bij online platformen is – meer gericht op ranking algoritmen – ook terug te zien in een position paper van de Duitse regering.<sup>143</sup> Daarin wordt gesteld dat platformen hun gebruikers moeten informeren over de manier waarop zij content voorselecteren en presenteren, bijvoorbeeld in een nieuwsfeed op een sociale media site (Beuth 2016). De Italiaanse regering nam in 2015 een verklaring van internetrechten aan, de verklaring is niet juridisch bindend maar dient vooral om de regering en het parlement aan te sporen om de opgestelde principes te respecteren (Pollicino & Bassini 2015). Tot slot wordt er ook in relatie tot specifieke technologische ontwikkelingen nagedacht over bepaalde ethische impacts. De Duitse minister van Transport heeft een ethische commissie ingesteld voor zelfrijdende auto's (Ramthun & Schlesiger 2016). en in de Verenigde Staten heeft de federale regering regels opgesteld voor (sterk) geautomatiseerde voertuigen, waarin aandacht gevraagd wordt voor ethische vraagstukken (USDoT 2016).

---

<sup>139</sup> [libdems.org.uk/protecting-your-data-online-with-a-digital-rights-bill](http://libdems.org.uk/protecting-your-data-online-with-a-digital-rights-bill)

<sup>140</sup> [cybersalon.org/digital-bill-of-rights-uk/](http://cybersalon.org/digital-bill-of-rights-uk/)

<sup>141</sup> Het recht op data-portabiliteit omvat niet alleen persoonlijke gegevens maar ook data geassocieerd met de account:

- "all files posted online by the consumer";

- "all data resulting from the use of the consumer's account . . ."; and

- "other data associated with the consumer's account the recovery of which is relevant to change supplier within a given industry".

<sup>142</sup> [republique-numerique.fr/pages/digital-republic-bill-rationale](http://republique-numerique.fr/pages/digital-republic-bill-rationale)

<sup>143</sup> [bmwi.de/DE/Presse/pressemitteilungen,did=764540.html](http://bmwi.de/DE/Presse/pressemitteilungen,did=764540.html)

**Tabel 4** Activiteiten binnen het politiek-bestuurlijk domein op het gebied van beleidsvorming.

Wie/wat	Technologie	Issue	Actie
<i>Ministerie van Economische Zaken</i>			
Visie Telecommunicatie	Internet, digitale communicatie	Vrij, open internet, keuzevrijheid	Stimuleren van veiligheid, neutraliteit en continuïteit
Brief big data en profilering	Big data, profilering, algoritmen	Privacy en gelijke behandeling	High level expert group
Brief toekomstbestendige regelgeving	Digitale platformen	Publieke waarden zoals consumetenveiligheid, eerlijke concurrentie	Experimenteerruimte in regelgeving met oog voor publieke waarden.
Brief ethische aspecten van het innovatiebeleid	Digitalisering	Versmelting mens & tech; privacy en autonomie	Aandacht voor ethiek in onderzoek; jaarlijkse rapportage bedrijvenbeleid
<i>Ministerie van Veiligheid en Justitie</i>			
Commissie Brouwer-Korf	Digitalisering, digitale communicatie	Veiligheid en privacy	Meldplicht datalekken; uitbreiding boetebevoegdheid AP
Notitie vrijheid & veiligheid in de digitale samenleving	Digitalisering, digitale communicatie	Veiligheid en privacy	Stimuleren privacy by design, verplichte PIA voor nieuwe wetgeving, campagne voor digitale weerbaarheid. Aanvraag WRR advies big data
Wetsvoorstel computercriminaliteit III	Digitalisering	Veiligheid	Nieuwe bevoegdheden veiligheidsdiensten
Kabinetsstandpunt encryptie	Encryptie	Vertrouwelijke communicatie, privacy	Wettelijke beperking op encryptie niet wenselijk
<i>Ministerie van Onderwijs Cultuur en Wetenschap</i>			
Brief Onderwijs 2032	Digitalisering, robotisering	Digitale vaardigheden, privacy, veiligheid, online omgangsvormen	Digitale geletterdheid in het kerncurriculum van het onderwijs. Continue scholing.
<i>Ministerie van Sociale Zaken en Werkgelegenheid</i>			
Brief Technologische ontwikkelingen en arbeidsmarkt	Robotisering, automatisering	Menselijke waardigheid, technologische werkeloosheid	Aanvraag onderzoek Rathenau, SER, CPB
Brief Werken aan de robotsamenleving	Robotisering, automatisering	Menselijke waardigheid, technologische werkeloosheid	Inzetten op goede opleidingen, leven lang leren, omscholing en transities.
<i>Ministerie van Buitenlandse Zaken</i>			
Brief Buitenlands internetbeleid	Internet	Fundamentele rechten: vrijheid, privacy, gelijkheid	Interdepartementale visie op internetbeleid, fundamentele rechten gelden ook online.

Mensenrechten-rapportage 2015	Internet, algoritmen	Fundamentele rechten: vrijheid, privacy, gelijkheid	Aandacht voor digitale rechten, ethiek en algoritmen op GCCS Conferentie
Brief Autonome wapensystemen	Autonome wapensystemen	Menselijke waardigheid, controle over technologie	Toewijzing verantwoordelijkheid onderdeel van ontwerpfase. AIRCW toetsing op betekenisvolle controle
<i>Ministerie van Binnenlandse Zaken en Koninkrijksrelaties</i>			
Brief iOverheid	Digitalisering van de overheid	Weerbaarheid burgers, controle over technologie	Besef impact digitalisering verankeren bij de overheid
Wetsvoorstel Wiv	Digitalisering communicatie	Veiligheid	Nieuwe bevoegdheden veiligheidsdiensten
<i>Parlement</i>			
Kamervragen en moties	Verschillende deelaspecten digitalisering	Verschillende ethische kwesties, veel aandacht voor privacy	Vragen om visie, standpunten, beleid, wet en regelgeving
VVD Robotagenda	Robotisering	Menselijke waardigheid; werkeloosheid	Inzetten op educatie. Onderzoek waarde van een Nationale Ethiek Commissie
D66 Techvisie	Digitalisering, internet	Privacy, surveillance, netneutraliteit, veiligheid, vertrouwelijke communicatie	Minister van Economie, Technologie en Privacy, digitale vaardigheden, versterking toezichhouders, zorgplicht internetreuzen
<i>EU en internationaal</i>			
EU – Onlife initiative	Digitalisering breed	Breed aantal ethische vraagstukken	Onlife Manifesto informeert onderzoeksagenda
EU – Algemene Verordening Gegevensbescherming	Dataverzameling en bescherming	Privacy, databescherming, transparantie	Versterking toezichthouder. Versterking rechten internetgebruiker en plichten dataverwerker
European Parliament – Draft Report on Civil Law rules on Robotics	Robotisering en kunstmatige intelligentie	Veiligheid, privacy, integriteit, menselijke waardigheid en autonomie	Voorstel voor een resolutie voor het Europees Parlement om ethische principes en een Europees Agentschap voor robotica en AI te creëren
Verenigd Koninkrijk – Campagne voor Digital Bill of Rights	Digitalisering, internet, digitale communicatie	Privacy, surveillance, machtsverhoudingen	Voorstel voor recht op eigenaarschap gegevens. Gelijke toegang internet

Frankrijk – Wetsvoorstel Republique Numerique	Digitalisering, internet, platformen digitale communicatie	Privacy, netneutraliteit, transparantie, machtsverhoudingen	Recht om vergeten te worden. Transparantie over verdienmodellen platformen. Rechten op data na overlijden
---	--	---	---

Rathenau Instituut

## Beleidsuitvoering

In de fase van beleidsuitvoering kijken we naar de manier waarop toezichthouders en toetsingscommissies ervoor zorgen dat de regels, normen en wetten worden geïmplementeerd en nageleefd die in de fase van beleidsvorming en -bepaling zijn vastgelegd. Een toezichthouder is een door de overheid aangesteld, onafhankelijk en onpartijdig instituut dat toeziet op naleving van wet- en regelgeving door organisaties. Toetsingscommissies voeren op basis van regelgevende kaders en protocollen meestal casus voor casus een toets uit of een bepaalde actie – zoals de aanschaf van een autonoom wapensysteem – zich aan de gestelde kaders houdt. Behalve bestuursrechtelijke controle kunnen organisaties ook via de juridische weg tot de orde worden geroepen, bijvoorbeeld door middel van collectieve acties. Deze paragraaf richt zich echter op toezichthouders en toetsingscommissies.

### Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens (AP), voorheen het College Bescherming Persoonsgegevens (CBP), ziet toe op de naleving van de privacywetgeving<sup>144</sup> en adviseert over nieuwe wet- en regelgeving. In de afgelopen jaren heeft de AP zich beziggehouden met thema's zoals profilering, het gebruik van gevoelige gegevens, en gegevensverwerking bij de overheid. Het gaf onder andere kritische adviezen over de gegevensverwerking bij wetsvoorstellen zoals de Wet maatschappelijke ondersteuning (Wmo), de Jeugdwet, de bewaarplicht telecomgegevens, en het concept-wetsvoorstel Computercriminaliteit III (CBP 2013; CBP 2014; AP 2015). De AP kijkt naar de noodzaak en onderbouwing van gegevensverwerking en of bevoegdheden zijn afgewogen tegen de inbreuken op de persoonlijke levenssfeer. Daarnaast tikt de AP verschillende organisaties op de vingers wanneer blijkt dat hun privacybeleid niet op orde is. Zo moest Google tijdens de herziening van de privacyvoorwaarden in 2014 ondubbelzinnige toestemming vragen voor het combineren van data uit verschillende diensten. Producenten van lifestyle-apps en wearables, zoals Nike+, worden er door de AP op gewezen dat gebruikers duidelijk moeten worden geïnformeerd over, en toestemming moeten geven voor het gebruik van hun gezondheidsgegevens.

In haar jaarverslag van 2014 geeft de AP aandacht aan big data en wordt gewezen op het gevaar van 'digitale predestinatie' wanneer mensen door profilering alleen maar keuzes aangeboden krijgen die binnen hun profiel passen (CBP 2014). Het thema big data krijgt op de agenda van 2015

<sup>144</sup> De vier belangrijkste wetten waarop de AP toezicht houdt zijn: Wet bescherming persoonsgegevens; Wet politiegegevens; Wet basisregistratie personen; Wet justitiële en strafvorderlijke gegevens.

vervolgens meer aandacht, en er wordt ook gesteld dat naast de principes van de wetgeving ook een breed maatschappelijk en politiek debat nodig is over big data (CBP 2015). De AP stelt dat de wereld de afgelopen vijf jaar op dit terrein ingrijpend is veranderd: door smartphones, wearables en Internet of Things ontkomen mensen er niet meer aan dagelijks ontelbare digitale sporen achter te laten. Dit roept de vraag op of de bescherming van persoonsgegevens 'dweilen met de kraan open' is geworden. De toezichthouder heeft echter vertrouwen dat de nieuwe maatregelen vanuit de Algemene Verordening Gegevensbescherming de controle van gebruikers zullen versterken (AP 2015:5).

De Wet Meldplicht datalekken, die op 1 januari ingegaan is, verplicht organisaties om datalekken direct te melden aan de AP. De AP heeft er dus een nieuwe taak als meldloket bijgekregen. De meldplicht heeft als doel om het beveiligingsniveau te verhogen en de zelfredzaamheid van burgers te vergroten. Tevens is de boetebevoegdheid van de AP versterkt. Dit geeft de AP mogelijkheid om zwaardere sancties op te leggen. De verwachting is dat dit een sterke preventieve werking heeft. De ontwikkelingen van big data, profilering, en het Internet of Things staan ook voor de komende jaren op de agenda. De focus van de maatregelen van de AP ligt in ervoor zorgen dat gebruikers correct worden geïnformeerd en om toestemming worden gevraagd. Een zorg op het gebied van profilering is dat dit vaak op onzichtbare manier gebeurt, waardoor de betrokkenen hier niet of moeilijk invloed op kunnen uitoefenen. Als onderwerp van onderzoek voor de komende periode noemt de AP onder andere dataverzameling over kinderen. De huidige generatie kinderen groeit op in een tijdperk van 'life-logging' waarbij grote hoeveelheden informatie over hun leven en ontwikkeling belanden in publieke en private databases. Voor ouders en kinderen is het belangrijk om te weten welke keuzes zij hierin kunnen maken (AP 2016).

### **Autoriteit Consument en Markt**

De Autoriteit Consument en Markt (ACM) houdt toezicht op mededinging, telecommunicatie en consumentenrecht. Een van de onderdelen van de agenda van de ACM is bescherming van de digitale consument, zodat die met vertrouwen kan internetten en online aankopen kan doen (ACM 2014; 2016a). De ACM onderzocht in dit kader hoe jongeren met hun online privacy omgaan en heeft een campagne gevoerd om het bewustzijn van online privacy te vergroten. Uit het onderzoek blijkt dat jongeren vaak niet weten dat apps geld verdienen aan hun persoonlijke gegevens. Om jonge consumenten hiervan bewust te maken, lanceerde de ACM de campagne 'Elke app heeft zijn prijs'.<sup>145</sup> Daarnaast handhaaft de ACM de vernieuwde cookieregels om consumenten bewust te informeren over online tracking.

In haar agenda van 2016 noemt de ACM ook de onderwerpen van netneutraliteit en de machtspositie van grote internetbedrijven. De ACM houdt in de gaten of internetaanbieders de, sinds april 2016 geldende, Europese plicht tot netneutraliteit respecteren (ACM 2016a). In een onderzoek naar de manier waarop effectief toezicht kan worden gehouden op online platformen stelt de ACM meer kennis nodig is over het functioneren van de dynamische markten waarin online platforms opereren. Naast kennisopbouw is het belangrijk om ook het contact met marktpartijen te

---

<sup>145</sup> [jaarverslag.acm.nl/jaarverslag-2015/campagne-elke-app-heeft-een-prijs](http://jaarverslag.acm.nl/jaarverslag-2015/campagne-elke-app-heeft-een-prijs)



versterken om meer inzicht te krijgen in verdienmodellen en strategieën en om ook in een vroegtijdig stadium bij te kunnen sturen (ACM 2016b).

### **College voor de Rechten van de Mens**

Het College voor de Rechten van de Mens (CRcdM) heeft tot doel in Nederland de rechten van de mens – waaronder het recht op gelijke behandeling – te beschermen, het bewustzijn van deze rechten te vergroten en de naleving van deze rechten te bevorderen.<sup>146</sup> Het beschermen van het recht op gelijke behandeling heeft een bijzondere plaats in de taken van het CRvdM. Het College heeft de taken overgenomen van de Commissie Gelijke Behandeling en kan individueel oordelen in het geval van discriminatie. In het voorgaande hebben we op verschillende plekken vragen gezien hoe technologische ontwikkelingen grond- en mensenrechten raken, zoals bij de high level expert group in zijn onderzoek naar de impact van big data op het recht op gelijke behandeling en bescherming van de persoonlijke levenssfeer. Het College stelt in een advies over het conceptwetsvoorstel voor de Wet op de inlichtingen en veiligheidsdiensten vragen bij de impact van de uitgebreide bevoegdheden tot gegevensverzameling op het recht op privacy. In zijn strategisch plan refereert het CRvdM niet aan de manier waarop technologische ontwikkelingen aan mensenrechten raken (CRvdM 2016). In een gesprek met het College wordt aangegeven dat de impact van technologische ontwikkeling wel ter sprake is gekomen in het kader van de strategische agenda, maar dat de focus op andere prioriteiten is gelegd.<sup>147</sup>

### **Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten**

De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) houdt toezicht op het handelen van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). De CTIVD waakt zodoende over ‘de balans tussen het belang van onze nationale veiligheid en dat van de bescherming van de persoonlijke levenssfeer van de burger’ (CTIVD 2016:2). De CTIVD onderzoekt de rechtmatigheid van operaties en dataverzameling door veiligheidsdiensten, en wordt ingeschakeld als onafhankelijke adviescommissie bij klachten over het handelen van de veiligheidsdiensten.

De invloed van digitalisering op het werkveld van de veiligheidsdiensten is een belangrijk onderwerp voor de CTIVD. In 2014 doet de commissie bijvoorbeeld onderzoek naar online informatieverzameling door de AIVD. Ze concludeert dat de dataverzameling en het gebruik van bepaalde bevoegdheden (zoals hacken) niet altijd goed gemotiveerd en verantwoord is, en doet aanbevelingen voor betere bestuurlijke controlemechanismen. Bij de wijziging van de Wet op de inlichtingen en veiligheidsdiensten (Wiv) pleit de CTIVD voor een versterking van het toezicht als waarborg voor de uitbreiding van de interceptiebevoegdheden in de Wiv. Een onafhankelijke instantie moet bindend in kunnen grijpen om onrechtmatige activiteiten te voorkomen of te laten stopzetten (CTIVD 2016).

Tot slot kijkt de CTIVD ook naar mogelijkheden om transparantie in het veiligheidsdomein te versterken – waar dat op een verantwoorde manier mogelijk is – om het vertrouwen in de

---

<sup>146</sup> Wet College voor de Rechten van de Mens (Staatsblad 2011, 573)

<sup>147</sup> Gesprek Jan Peter Loof, 11-05-2016

informatieverzameling door veiligheidsdiensten te versterken en het ontstaan van mythes en misverstanden tegen te gaan. Ze startte in 2016 een onderzoek naar notificatie en inzage bij veiligheidsdiensten. De commissie beschikt over veel expertise, maar stelt: 'In deze tijd van big data en van digitalisering van het inlichtingenwerk is meer nodig' (CTIVD 2015: 3). Vanaf 2014 is daarom een kenniskring van externe deskundigen ingesteld om – in visievorming en onderzoek – sterker in verbinding te staan met technische ontwikkelingen en maatschappelijke en wetenschappelijke discussies.

### **Overige toezichthouders en toetsingscommissies**

Het Nationaal Cyber Security Centrum reageert op cyberdreigingen en incidenten en werkt aan het versterken van een veilige en weerbare digitale samenleving. Belangrijk focuspunt is de bescherming en continuïteit van de vitale infrastructuur (bijvoorbeeld energie-, water- en telecomsector), zodat de Nederlandse samenleving goed kan blijven functioneren. Daarnaast zet het NCSC zich in om het bewustzijn en capaciteiten op het gebied van informatieveiligheid en privacy te versterken bij burgers, bedrijven en overheden. De Cyber Security Raad ziet toe op de uitvoering van de Nationale Cyber Security Strategie en zorgt voor bewustwording van nieuwe onderwerpen. De ontwikkeling van het Internet of Things is een van de onderwerpen waar de Cyber Security Raad zich vanuit het cybersecurity perspectief de komende jaren in zal verdiepen (CSR 2016).

De Adviescommissie Internationaal Recht en Conventioneel Wapengebruik geeft advies over het verwerven, bezit en gebruik van wapens en kijkt naar de mate waarin dit verenigbaar is met het internationaal humanitair oorlogsrecht. De commissie speelt ook een rol in het adviseren over het aanschaf van autonome wapentechnologie en evalueert of daarbij sprake is van betekenisvolle menselijke controle.

De Nationale Ombudsman staat burgers bij wanneer zij problemen hebben met de overheid. Een van de thema's op de agenda van de Ombudsman is digitalisering. De Ombudsman stelt dat digitalisering voor veel gebruiksgemak kan zorgen bij burgers, maar ook voor situaties kan zorgen waar systemen in de fout gaan, gegevens niet kloppen of misbruikt worden door anderen. Daarnaast maakt de Ombudsman zich hard voor mensen die niet digitaal vaardig zijn en daardoor buitengesloten dreigen te raken in de steeds verder digitaliserende communicatie met de overheid.

### **Internationale ontwikkelingen**

#### *EDPS adviesgroep over digitale ethiek*

De European Data Protection Supervisor (EDPS) is de Europese toezichthouder voor gegevensbescherming. De EDPS adviseert de Europese Commissie en het parlement over wetgeving en beleid met betrekking tot privacy en gegevensbescherming, en werkt samen met nationale toezichthouders om tot uniforme Europese gegevensbescherming te komen.

De EDPS heeft een actieve rol gespeeld in de totstandkoming van de Algemene Verordening Gegevensbescherming (EU 2016/679), waarin nieuwe maatregelen zijn genomen om de bescherming van persoonsgegevens te versterken. Eind 2015 publiceerde de EDPS de opinie *Towards a new digital ethics*, waarin de toezichthouder aandacht vraagt voor de rol van

technologische ontwikkelingen, zoals algoritmes, AI, big data en het Internet of Things (EDPS 2015). Het is moeilijk voor het individu om zich nog te onttrekken aan dataverzameling, surveillance door overheden lijkt zich steeds verder uit te breiden en profilering zorgt voor risico's van stigmatisering en buitensluiting. Het leidt tot de vraag of mensen nog de vrijheid hebben om zichzelf vrij te ontwikkelen zonder geïdentificeerd en geprofileerd te worden. De huidige principes van gegevensbescherming alleen zijn volgens de EDPS niet meer voldoende om menselijke waardigheid online te beschermen. De EDPS wil dat er meer aandacht komt voor de ethische dimensie van gegevensverwerking, met oog voor de impact van data op vrijheid, waardigheid en het functioneren van democratische processen. Daarbij vindt de adviesgroep vier punten van belang: 1) toekomstbestendige regelgeving; 2) verantwoordelijkheid bij organisaties die data verwerken; 3) privacy bewustzijn bij ingenieurs en programmeurs die software ontwikkelen; en 4) empowerment van het individu om zelf beslissingen te kunnen nemen over zijn gegevens. Daarnaast stelt de EDPS ook een ethische adviesgroep in om de verhouding tussen mensenrechten, digitale technologie en businessmodellen in de eenentwintigste eeuw te verkennen. De stap naar digitale ethiek vraagt ook om reflectie op de rol van de toezichthouder en de principes waarmee zij haar werk vormgeeft. De komende jaren wil de EDPS meer vanuit het perspectief van verantwoordelijk handelen kijken in plaats van het 'mechanisch opvolgen van de letter van de wet' (EDPS 2015a: 11). Niet alleen het inhoudelijke vraagstuk over ethische uitdagingen staat dus op de agenda, maar ook de governancevraag naar het organiseren van toezicht en het mandaat van de toezichthouder.

**Tabel 5** Activiteiten binnen het politiek-bestuurlijk domein op het gebied van beleidsuitvoering.

Wie/wat	Technologie	Issue	Actie
AP	Digitalisering (diensten die persoonlijke gegevens verwerken)	Privacy, gegevensbescherming	Toezicht gegevensverwerking overheid en bedrijfsleven
ACM	Internet, apps	Privacy, machtsverhoudingen	Bewustwordingcampagne privacy, macht internetaanbieders
CRvdM	-	Mensenrechten (speciale aandacht discriminatie)	-
CTIVD	Veiligheidstechnologie	Privacy, gegevensbescherming, veiligheid	Toezicht op veiligheidsdiensten
NCSC / CSR	Digitalisering	Veiligheid	Stimuleren veilige en weerbare digitale samenleving
AIRCW	Wapentechnologie	Autonomie, controle over technologie, menselijke waardigheid	Advies over betekenisvolle menselijke controle bij wapensystemen
Nationale ombudsman	Digitale	Autonomie, menselijke	Klachten bij systemen

	overheidsdiensten	waardigheid	van de digitale overheid die in de fout gaan
<i>EU en internationaal</i>			
EDPS	Digitalisering (diensten die persoonlijke gegevens verwerken)	Verbreiding van privacy naar autonomie, menselijke waardigheid, discriminatie	Adviesgroep digitale ethiek, verkenning impact van digitalisering op mensenrechten

## Bibliografie

ACM (2014) ACM Agenda 2014-2015. Den Haag: ACM. Online beschikbaar: [acm.nl/nl/organisatie/missie-visie-strategie/onze-agenda/acm-agenda-2014-2015/](http://acm.nl/nl/organisatie/missie-visie-strategie/onze-agenda/acm-agenda-2014-2015/)

ACM (2016a) ACM Agenda 2016-2017. Den Haag: ACM. Online beschikbaar: [acm.nl/nl/organisatie/missie-visie-strategie/onze-agenda/acm-agenda-2014-2015/](http://acm.nl/nl/organisatie/missie-visie-strategie/onze-agenda/acm-agenda-2014-2015/)

ACM (2016b) Grote platforms, grote problemen? Een beschouwing van online platforms vanuit Mededingingsperspectief. Den Haag: ACM

AIV (2012) Digitale oorlogsvoering. No 77, AIV/No 22, CAVV December 2011. Den Haag: Adviesraad Internationale Vraagstukken.

AIV (2014) Het Internet. Een wereldwijde vrije ruimte met begrensde staatsmacht. No. 92. Den Haag: Adviesraad Internationale Vraagstukken.

AIV (2015) Autonome Wapensystemen. De noodzaak van betekenisvolle menselijke controle. No. 97 AIV / No. 26 CAVV. Den Haag: Adviesraad Internationale Vraagstukken.

AP (2015) *Jaarverslag 2015*. Den Haag: Autoriteit Persoonsgegevens.

AP (2016) *AP Agenda 2016*. Den Haag: Autoriteit Persoonsgegevens.

Article 29 Data Protection Working Party and the Working Party on Police and Justice (2011) *The Future of Privacy*. WP 168

Bennet, C.J. & C. Raab (2006) *The governance of privacy: Policy instruments in global perspective*. Massachusetts: MIT Press.

Beuth, P (2016) Bundesregierung will mehr über Googles Algorithmus wissen. In: *Die Zeit*, 13-05-2016. Online beschikbaar: <http://www.zeit.de/digital/internet/2016-05/transparenz-algorithmen-bundesregierung-google-facebook/komplettansicht>

Bits of Freedom (2015) *Jaarverslag 2015. Connected we stand*. Amsterdam: Bits of Freedom.

Boka (2016) Facebooks Research Ethics Board Needs to Stay far Away from Facebook. In: *Wired*, 23 juni 2016. Online beschikbaar: [wired.com/2016/06/facebook-research-ethics-board-needs-stay-far-away-facebook](http://wired.com/2016/06/facebook-research-ethics-board-needs-stay-far-away-facebook)

CBP (2013) *Jaarverslag 2013: Het CBP in zich.*, Den Haag: College Bescherming Persoonsgegevens.

CBP (2014) *Jaarverslag 2014: Het CBP in zicht*. Den Haag: College Bescherming Persoonsgegevens.

CBP (2015) *CBP Agenda 2015*. Den Haag: College Bescherming Persoonsgegevens.

CPB (2014) *Kiezen voor Privacy: Hoe de markt voor persoonsgegevens beter kan*. CPB Policy Brief, Den Haag: CPB

College voor de Rechten van de Mens (2016) *Strategisch Plan 2016-2019*, Utrecht: College voor de Rechten van de Mens.

Commissie Franken (2000) *Commissie grondrechten in het digitale tijdperk*. Den Haag.

Consumentenbond (2015) *Jaarverslag 2015*. Den Haag: Consumentenbond.

CTIVD (2015) *Jaarverslag 2014-2015*. Den Haag: Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten.

CTIVD (2016) *Jaarverslag 2015*. Den Haag: Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten.

Cyber Security Raad (2016) *Werkprogramma 2016*. De toekomst is dichtbij dan je denkt. Den Haag: CSR.

D66 (2016) *Concept-verkiezingsprogramma. Samen sterker - kansen voor iedereen*. Den Haag: D66.

Digital Government Review (2014) *Making Digital Government Work for Everyone*. 25-11-2014. Digital Government Review.

Dommering, E.J. (2011) Een nieuw voorstel tot aanpassing van de Grondwet. *Computerrecht 2*, pp. 52-55.

Dratwa, J. (Ed.) (2014) *Ethics of Security and Surveillance Technologies. Opinion No. 28 of the European Group on Ethics in Science and New Technologies*. Brussels, 20 mei 2014.

EC (2013) *The Onlife Manifesto: Being Human in a Hyperconnected Era*. [ec.europa.eu/digital-single-market/sites/digital-agenda/files/Manifesto.pdf](http://ec.europa.eu/digital-single-market/sites/digital-agenda/files/Manifesto.pdf)

ECP (2015) *De volwassen informatiesamenleving. Het nieuwe normaal*. Visiedocument ECP. December 2015.

EDPS (2015) *Towards a new digital ethics: Data dignity and technology. Opinion 4/2015*, Brussel : European Data Protection Supervisor.

EDPS (2015a) *Leading by Example: The EDPS strategy 2015-2019* Brussel: European Data Protection Supervisor.

EDPS (2016) *EDPS starts work on a New Digital Ethics*. EDPS/2016/05, Brussel, 28 januari 2016 Press Release.

EDRI (2014) *The Charter of Digital Rights. The EDRI papers 10*, Brussel: European Digital Rights initiative.

Eskens, S., J. Timmer, L. Kool & R. van Est (2016) *Beyond Control: Exploratory study on the discourse in Silicon Valley about consumer privacy in the Internet of Things*, Den Haag: Rathenau Instituut.

Est, R van (2014) *Intieme technologie: De slag om ons lichaam en gedrag*, Den Haag: Rathenau Instituut.

Est, R. van, D. Stemerding, V. Rerimassie, M. Schuijff, J. Timmer & F. Brom (2014) *From Bio to NBIC convergence – From medical practice to daily life; Report written for the Council of Europe, Committee on Bioethics*, Den Haag: Rathenau Instituut.

Est, R. van & L. Kool (red.) (2015) *Werken aan de robotsamenleving. Visies en inzichten uit de wetenschap over de relatie technologie en werkgelegenheid*, Den Haag: Rathenau Instituut.

Est, R. van & V. Rerimassie (2014) *Strijd om onze intimiteit. Het Bericht*, Den Haag: Rathenau Instituut.

Est, van R. & D. Stemerding (2012) *Making Perfect Life: Final Report. European Governance Challenges in 21st Century Bio-engineering*, Brussel: STOA

Forus, A. (2014) Preface Committee on Bioethics of the Council of Europe by Chair DH-BIO. In: R. van Est, D. Stemerding, V. Rerimassie, M. Schuijff, J. Timmer & F. Brom (2014) *From Bio to NBIC convergence – From medical practice to daily life; Report written for the Council of Europe, Committee on Bioethics*, Den Haag: Rathenau Instituut.

GCIG (2016) *Our Internet. Global Commission on Internet Governance*, Ontario / London: Centre for International Governance Innovation / Chatham House.

Geesink, I., M. Heerings & S. van Egmond (red.) (2016) *De meetbare mens: Het digitaal meten van het zieke en gezonde lichaam*, Den Haag: Rathenau Instituut

Gezondheidsraad (2006) *Betekenis van nanotechnologieën voor de gezondheid*, Den Haag: Gezondheidsraad; publicatie nr. 2006/06. ISBN 90-5549-593-X

Hof, C. van 't, J. Timmer & R. van Est (red.) (2012a) *Voorgeprogrammeerd: Hoe internet ons leven leidt*, Boom Lemma.

Hof, C. van 't, J. Timmer & R. van Est (2012b) *Het Bericht: Voorgeprogrammeerd – Online keuzevrijheid onder druk*, Den Haag: Rathenau Instituut.

IEEE (2016) *The Global Initiative for Ethical Consideration in the Design of Autonomous Systems*. IEEE. Online beschikbaar: [standards.ieee.org/develop/indconn/ec/ec\\_about\\_us.pdf](https://standards.ieee.org/develop/indconn/ec/ec_about_us.pdf)

Janssen, A., L. Kool & J. Timmer (2015) *Dicht op de huid. Gezichts- en emotieherkenning in Nederland*, Den Haag: Rathenau Instituut

Kiss, J. (2014) An online Magna Carta: Berners-Lee calls for bill of rights for web. In: *The Guardian*, 12-03-2014. Online beschikbaar: [theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web](https://www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web)

Kool, L., J. Timmer & R. van Est (2013) *Keuzes voor de e-coach: Maatschappelijke vragen bij de automatisering van de coachingspraktijk*. Den Haag: Rathenau Instituut.

Kool, L., J. Timmer & R. van Est (2015) *De data-gedreven samenleving: een achtergrondstudie*. Den Haag: Rathenau Instituut

Kool, L., J. Timmer & R. van Est (red.) (2014) *Eerlijk advies: De opkomst van de e-coach*. Den Haag: Rathenau Instituut.

Koops, E.J. (2011) Digitale grondrechten en de Staatscommissie: op zoek naar de kern. In: *Tijdschrift voor Constitutioneel Recht*, 2 (2), p.168-185.

Kreijveld, M., J. Deuten & R. van Est (red.) (2014) *De kracht van platformen: Nieuwe strategieën voor innoveren in een digitale wereld*. Den Haag/Deventer: Rathenau Instituut/Vakmedianet.

Ladikas, M., S. Chaturvedi, Y. Zhao, & D. Stemerding (red.) (2015) *Science and technology governance and ethics: A global perspective from Europe, India and China*. Heidelberg u.a.: Springer Open 2015, pp. 1-8.

Lucas, A. (2016) *Robotisering zonder achterblijvers*. Den Haag: VDD

Martijn, M. (2016) Deze professor probeert privacy opnieuw uit te vinden en dat is broodnodig. In: *De Correspondent*, 8 augustus 2016. Online beschikbaar: [decorrespondent.nl/5043/Deze-professor-probeert-privacy-opnieuw-uit-te-vinden-en-dat-is-broodnodig/155102508-199b13c9](https://decorrespondent.nl/5043/Deze-professor-probeert-privacy-opnieuw-uit-te-vinden-en-dat-is-broodnodig/155102508-199b13c9)

Messer, P. (red.) (2012) *Robotrevolutie vraagt om actie. Het Bericht*. Den Haag: Rathenau Instituut.

Mulgan (2016) *A machine intelligence commission for the UK: how to grow informed public trust and maximise the positive impact of smart machines*, London: Nesta.



Moerel, L. (2015) Zo behouden alleen de rijken hun privacy. In: *NRC Handelsblad*, 28 november 2015. Online beschikbaar: [nrc.nl/nieuws/2015/11/28/zo-behouden-alleen-de-rijken-hun-privacy-1561104-a579887](http://nrc.nl/nieuws/2015/11/28/zo-behouden-alleen-de-rijken-hun-privacy-1561104-a579887)

Munnichs, G. & J. Bos (2016) *Digitalisering van dieren: Verkenning Precision Livestock Farming*. Den Haag: Rathenau Instituut.

Nanopodium (2011) *Verantwoord verder met nanotechnologie. Bevindingen maart 2009 – januari 2011*, Eindrapport Commissie Maatschappelijke Dialoog Nanotechnologie. Amsterdam: Nanopodium

NJV (2016) Homo Digitalis. In: *Handelingen Nederlandse Juristen-Vereniging 146*, Alphen aan de Rijn: Wolters-Kluwer.

Noort, W. van (2016) We bouwen aan een dictatuur van data. In: *NRC Handelsblad*, 19 augustus 2016. Online beschikbaar: [nrc.nl/nieuws/2016/08/19/we-bouwen-aan-een-dictatuurvan-data-3869694-a1517117](http://nrc.nl/nieuws/2016/08/19/we-bouwen-aan-een-dictatuurvan-data-3869694-a1517117)

Nouwt, J., P.H. Blok, B.J. Koops, M.H.M. Schellekens, E. Schreuders & M. de Vries (2000) Grondrechten in het digitale tijdperk. In: *Nederlands Juristenblad 75(27)*, pp. 1321-1327.

Onderwijsraad (2015) *Meerjarenagenda 2015–2020, werkprogramma 2016*. Den Haag: Onderwijsraad.

Pollicino, O. & M. Bassini (2015) *An Internet Bill of Rights? Pros and cons of the Italian way*. *London School of Economics – Media Policy Project Blog*. Online beschikbaar: [blogs.lse.ac.uk/mediapolicyproject/2015/08/05/an-internet-bill-of-rights-pros-and-cons-of-the-italian-way](http://blogs.lse.ac.uk/mediapolicyproject/2015/08/05/an-internet-bill-of-rights-pros-and-cons-of-the-italian-way)

Prins, J.E.J. (2015) Grondrechten en digitalisering. In: *Nederlands Juristen Blad 2015/403*, afl. 8, p. 419.

Privacy First (2015) *Eigen keuzes in een vrije omgeving. Jaarverslag 2015*. Amsterdam: Privacy First.

Raad voor de Rechtspraak (2014) *Advies grondwetswijziging recht op eerlijk proces*. Den Haag: Raad voor de Rechtspraak.

Radboud Universiteit (2016) Bart Jacobs zet digitale beveiliging op de kaart. Online beschikbaar: [ru.nl/onderzoek/over/vm/onderzoeksthema/informatica-digitale/vm/professor-bart](http://ru.nl/onderzoek/over/vm/onderzoeksthema/informatica-digitale/vm/professor-bart)

Rli (2015a) *Werkprogramma 2015-2016*. Den Haag: Raad voor de leefomgeving en infrastructuur.

Rli (2015b) *Verkenning technologische innovaties in de leefomgeving*. Den Haag: Raad voor de leefomgeving en infrastructuur.

Rli (2016) *Werkprogramma 2016-2017*. Den Haag: Raad voor de leefomgeving en infrastructuur.

Royakkers, L., F. Daemen & R. van Est (2012) *Overal robots. Automatisering van de liefde tot de dood*. Den Haag: Boom Lemma.

Royakkers, L. & R. van Est (2016) *Just ordinary robots: Automation from love to war*. Boca-Raton, FL: CRC Press.

Salvi, M. (red.) (2012) *Ethics of information and communication technologies. European Group on Ethics in Science and New Technologies to the European Commission. Opinion No 26*. Brussel, 22 februari 2012.

Shead, S. (2016) The biggest mystery in AI right now is the ethics board that Google set up after buying DeepMind. *Business Insider*, 26 maart 2016. Online beschikbaar: [uk.businessinsider.com/google-ai-ethics-board-remains-a-mystery-2016-3](http://uk.businessinsider.com/google-ai-ethics-board-remains-a-mystery-2016-3)

Solove, D.J. (2002) Conceptualizing Privacy. In: *California Law Review* 2002(4), pp. 1087-1156.

Ten Oever, N. & C. Cath (2016) Research into Human Rights Protocol Considerations. Internet Draft. IETF. Online beschikbaar: [tools.ietf.org/pdf/draft-tenoever-hrpc-research-04.pdf](http://tools.ietf.org/pdf/draft-tenoever-hrpc-research-04.pdf)

Timmer, J., I. Elias, L. Kool & R. van Est (2015) *Berekende risico's: Verzekeren in de data-gedreven samenleving*. Den Haag: Rathenau Instituut

Timmer, J. & L. Kool (red.) (2014) *Ter de Robotauto: De zelfsturende auto voor publieke doelen*. Den Haag: Rathenau Instituut.

Timmer, J., J. Smids, L. Kool, A. Spahn & R. van Est (2013) *Op advies van de auto: Persuasieve technologie en de toekomst van het verkeerssysteem*. Den Haag: Rathenau Instituut

Verhey, L.F.M. (2011) Grondrechten in het digitale tijdperk: driemaal is scheepsrecht? In: *Tijdschrift voor Constitutioneel Recht*, 2(2), pp.152-167.

Verbond van Verzekeraars (2016) *Grip op data*. Green Paper Big data. Den Haag: Verbond van Verzekeraars.

Verhoeven, K., M. van Vliet, N. Mastenbroek, M. van Dieijen, D. van Egmond & O. Arts (2016) *Techvisie D66*. Den Haag: D66.

Whittall, H., L. Palazzani, M. Fuchs & Gzásó, A. (Conference's rapporteurs to the Committee on Bioethics) (2015) *Report of the International conference on Emerging technologies and human rights. Strasbourg, 4-5 May 2015*. Strasbourg: Council of Europe, DH-BIO.

WRR (2011) *iOverheid*. Rapport 86. Amsterdam: Amsterdam University Press.

WRR (2015) *De publieke kern van het internet. Naar een buitenlands internetbeleid*. Rapport 94. Amsterdam: Amsterdam University Press

WRR (2015) *De robot de baas. De toekomst van werk in het tweede machinetijdperk*. Verkenning 31. Amsterdam: Amsterdam University Press.

WRR (2016) *Big Data in een vrije en veilige samenleving*. Rapport 95. Amsterdam: Amsterdam University Press.

Zoeteman, C. & I. Widdershoven-Heerding (2007) Bio-ethiek: uniformiteit of maatwerk? COGEM Jaarverslag 2006, pp. 30-33.

# Appendix B: De betekenis van publieke governance

*Governance is about efforts to align or bring about concerted action across multiple, competing institutional modes of social coordination for public purpose (O'Toole 2000: 278).*

## Governance als maatschappelijke sturing

Etymologisch is het begrip 'governance' verwant aan het Griekse *kubernein*, dat het besturen van een boot of wagen betekent. De filosoof Plato was de eerste die het woord gebruikte om te spreken over het bewust sturen van het handelen van grote groepen mensen om daarmee gewenste resultaten te verkrijgen en risico's en ongewenste uitkomsten te vermijden (Hoppe 2010, 10). Bij publieke governance gaat het dus in essentie om maatschappelijk sturen. Governance is een meerduidig concept en het is eenvoudig om de weg kwijt te raken in de omvangrijke literatuur daarover. Hieronder introduceren we een aantal inzichten en begrippen uit die literatuur dat behulpzaam kan zijn bij het nadenken over de governance van de maatschappelijke en ethische aspecten van wetenschap en technologie.

## Governance van publieke vraagstukken

Governance is gericht op het aanpakken van publieke vraagstukken. Het gaat hier om maatschappelijke problemen, oftewel problemen die slechts via collectieve actie opgelost kunnen worden (vgl. Hoppe 2010). Praktijken en processen van governance ontwikkelen zich zodoende rond bepaalde problemen en krijgen vormen in een gemeenschappelijke worsteling met politieke problemen en zoektocht naar mogelijke oplossingen. Daarbij spelen zowel de vrije maatschappelijke uitwisseling van argumenten als machtsuitoefening, met andere woorden rede en macht, een rol (Jaspers 1974).

Het gaat dus enerzijds om het vinden van en agenderen van problemen en anderzijds om het oplossen daarvan. Hoppe (2010, 17-18) onderscheidt daarbij drie processen: onderbouwen van het probleem, zoeken naar politieke steun en politieke participatie (in het Engels kort aangeduid met *puzzling, powering, participation*). In het eerste proces gaat het erom het betreffende probleem goed, bijvoorbeeld met behulp van wetenschappelijk kennis, te onderbouw en te bezien in hoeverre het hier inderdaad om een publiek probleem gaat dat om overheidsactie vraagt. Het tweede proces betreft het verkrijgen van politieke steun: kan er voldoende politieke druk en invloed gemobiliseerd worden om het probleem op de politieke en beleidsagenda te krijgen? Het probleem is namelijk in voortdurende competitie om de beperkte aandacht en probleemoplossend vermogen van de staat. Het derde proces betreft participatie: wie is betrokken of juist niet bij de definitie van het probleem en de bepaling van oplossingen, instrumenten en vormgeving van instituties? Welke publieke belangen of waarden zijn goed of minder goed gearticuleerd en vertegenwoordigd?

Vanuit het perspectief van de democratische rechtstaat dient governance aan een aantal voorwaarden te voldoen. Vanuit het besef dat er wereldwijd vele 'falende' of 'fragiele' staten zijn, ontwikkelende de Wereldbank in 1994 het begrip *good governance*: 'Governance is epitomized by

predictable, open, and enlightened policymaking (that is, transparent processes); a bureaucracy imbued with a professional ethos; an executive arm of government accountable for its actions; and a strong civil society participating in public affairs; and all behaving under the rule of law.' (World Bank 1994, vii). Deze definitie is nog steeds actueel. Centraal hierin staat hoe de overheid interacteert met de samenleving.

## Governance als de vormgeving van interactie tussen overheid en maatschappij

Het begrip governance impliceert dat de overheid niet als enige behartiger van publieke belangen gezien wordt en dat sturing van de samenleving niet alleen via formele instrumenten, zoals wet- en regelgeving, plaatsvindt. Publieke diensten worden geleverd door een netwerk van actoren uit de publieke en private sector (Van Kersbergen en Van Waarden 2001). Met andere woorden: de verantwoordelijkheden voor het leveren van publieke diensten zijn verspreid over een netwerk van publieke en private partijen. De overheid is een netwerkpartner en stuurt in interactie met andere partijen. Daarbij wordt gebruikgemaakt van een zeer diverse en uitgebreide mix van formele en informele praktijken. Naast traditionele vormen van dwang en *command & control*, kan het daarbij gaan om bijvoorbeeld stimulering van publiek debat, onderhandelingen, samenwerking, gezamenlijke visievorming en vorming van allianties (cf. Van Kersbergen & Van Waarden 2004: 151-152). Governance kan ook een reactie zijn op publiek verzet, gebrek aan draagvlak, institutioneel wantrouwen of de complexiteit van vraagstukken. In Nederland werkt de overheid al zeer lang samen met diverse actoren uit de samenleving. Maar de afgelopen decennia is de behoefte aan governance gegroeid vanwege digitalisering, privatisering en internationalisering (Hajer et al. 2004).

Er zijn diverse governance-begrippen in omloop die verwijzen naar bepaalde typen van interactie tussen de overheid en maatschappelijke actoren. Zo zijn er onder meer *multi-stakeholder governance* en *netwerk governance*. Bij multi-stakeholder governance komen actoren uit het bedrijfsleven, de maatschappij en de overheid samen om een gezamenlijk aanpak te ontwikkelen voor een kwestie die hen allen aangaat, maar die te complex is om zonder samenwerking op een effectieve wijze aan te pakken. Hierboven werd al verwezen naar internationalisering. Naast interactie tussen publieke en private actoren, vragen veel kwesties ook om overleg tussen diverse bestuurslagen, zoals Europees, nationaal, regionaal en lokaal. Deze bestuurlijke dynamiek wordt gevangen door de term *multi-level governance*: 'The sharing of policy-making competencies in a system of negotiation between nested governments at several tiers (supranational, national, regional and local) on the one hand and private actors (NGO's, producers, consumers, citizens, etc.) on the other' (Van Tatenhove & Liefferink, geciteerd in Hajer et al. 2004: 18). Daar waar het specifiek gaat om de interactie tussen overheidspartijen, burgers en maatschappelijke groepen wordt vaak de term *deliberatieve governance* gebruikt. Hierbij staan democratische waarden en de kwaliteit van de uitwisseling van visies en belangen centraal. Deliberatieve praktijken ontwikkelen zich veelal in reactie op de moeizame politiek-bestuurlijke omgang met gevoelige maatschappelijke problemen en wanneer er sprake is van een gebrekkige uitwisseling van argumenten en wederzijds wantrouwen (Hajer et al. 2004). Deliberatie kan dan een manier zijn om institutioneel vertrouwen op te bouwen en te zoeken naar werkbare oplossingen.

## Meta-governance van het governance-ecosysteem

Governance gaat dus over het collectief besturen van onze samenleving. Verwijzend naar de bovengenoemde originele betekenis van het woord, definieert Kooiman governance als een 'hypercomplex sociaal-cybernetisch systeem' (geciteerd in Blatter 2012, 14). Anders gezegd: het is niet meer van deze tijd om bij de governance van publieke problemen slechts naar het handelen van de overheid te kijken. Het is van belang om oog te hebben voor het gehele systeem aan governance-arrangementen in de samenleving om publieke problemen te onderkennen, te bespreken, te onderzoeken, te agenderen en daarvoor oplossingen te vinden en deze te implementeren en te evalueren. Om dat soort processen op een legitieme en effectieve manier te organiseren is vaak van belang dat de set aan instituties en bestuurlijke en maatschappelijke processen divers is. Tezamen vormen die een zogeheten governance-ecosysteem. Het governancevraagstuk gaat dan om de vraag of het governance-ecosysteem, als het geheel aan governance-arrangement rond een bepaald publiek probleem, goed werkt. Volgens Hoppe (2010) spelen bij het verbeteren van een governance-ecosysteem twee zoekprocessen een rol. Het eerste proces betreft de instituties. Zeker in het geval van nieuwe problemen is vaak sprake van een gebrek aan instituties. Hajer & Wagenaar (2003) spreken van een 'institutionele leegte', met een gebrek aan gedeelde normatieve kaders en organisatorische capaciteiten en onduidelijkheid over wie waar verantwoordelijk voor is. De socioloog Ulrich Beck spreekt in deze zin van 'georganiseerde onverantwoordelijkheid' (Beck 1988), die hij ziet als een sleutelkenmerk van onze hightech-ricisomaatschappij (Beck 1992). Het van onderaf opbouwen van instituties of het uitbouwen en verbeteren van bestaande instituties vereist onder meer institutioneel ondernemerschap. Hoppe (2004) spreekt in dat geval van *meta-governance* omdat het hier gaat om de governance van de governance van problemen, oftewel de inrichting van het governance-ecosysteem waarmee collectieve problemen benoemd en geadresseerd kunnen worden. Een tweede zoektocht betreft de organisatie van maatschappelijke betrokkenheid en afstemming met de belevingswereld van gewone burgers.

## Relevante vragen vanuit governanceperspectief

Bovenstaande korte introductie van het begrip governance levert tal van vragen op, zowel op het gebied van de governance van problemen als op het gebied van de meta-governance (de opbouw en werking van het governance-ecosysteem).

- Met betrekking tot de governance van problemen gaat het om vragen als:
- Welke publieke problemen zijn gesignaleerd?
- Welke belangen of waarden zijn goed of minder goed gearticuleerd?
- Hoe discussieren diverse actoren in de samenleving en politiek over deze problemen?
- Hoe zijn problemen al dan niet politiek geagendeerd?
- Welke partijen zijn betrokken geweest bij het debat en de vormgeving van beleid?
- Welke oplossingen zijn aangedragen en geïnstitutionaliseerd?

Met betrekking tot de meta-governance van problemen gaat het om vragen als:

- Welke instituties zijn er om te discussiëren over publieke problemen en deze politiek aan te kaarten?

- Op welke manieren vindt afstemming plaats tussen publieke en private actoren en tussen overheden en gewone burgers en maatschappelijke organisaties?
- Op welke wijze worden publieke waarden institutioneel geborgd?
- Welke instituties zijn er door de jaren heen opgebouwd om dat te doen?
- Hoe ziet het governance-ecosysteem rond een bepaalde kwestie er uit?

## Bibliografie

- Beck, U. (1988) *Gegengifte. Die Organisierte Unverantwortlichkeit*. Frankfurt/Main: Suhrkamp.
- Beck, U. (1992) *Risk Society. Towards a New Modernity*. London: Sage.
- Blatter, J. (2012) *Forms of political governance: Theoretical foundations and ideal types*. Lucerne: University of Lucerne.
- Hajer, M.A. & H. Wagenaar (red.) (2003) *Deliberative policy analysis: Understanding governance in the network society*. Cambridge: Cambridge University Press.
- Hajer, M.A., J.P.M. van Tatenhove & C. Laurent (2004) *Nieuwe vormen van governance: Een essay over nieuwe vormen van bestuur met een empirische uitwerking naar de domeinen van voedselveiligheid en gebiedsgericht beleid*. Bilthoven: RIVM.
- Hendriks, F. & F. Drosterij (2010) Goed bestuur in de stad: wat staat op het spel? In: *Bestuurskunde* 19(4), pp. 6-18.
- Hoppe, R. (2010) *The governance of problems: Puzzling, powering and participation*. Bristol: The Policy Press.
- Jaspers, K. (2012/1965) *Kleine Schule des philosophischen Denkens*. München: Piper.
- Kersbergen, K. van & F. van Waarden (2001) *Shifts in governance: Problems of legitimacy and accountability*. Den Haag: NOW.
- Kersbergen, K. van & F. van Waarden (2004) 'Governance' as a bridge between disciplines: Cross-disciplinary inspiration regarding shifts in governance and problems of governability, accountability and legitimacy. In: *European Journal of Political Research* 43, pp. 143-171.
- O'Toole, L.J. (2000) Research and policy implementation: Assessment and prospects. In: *Journal of Public Administration Research and Theory* 10, pp. 263-288.
- World Bank (1994) *Governance: The World Bank's experience*. Washington D.C.: World Bank.



## Appendix C: Geraadpleegde experts

Naam	Organisatie
Herm van der Beek	Ministerie van Economische Zaken
Arie van Bellen	ECP
Vincent Böhre	Privacy First
Frans Brom	Wetenschappelijke Raad voor het Regeringsbeleid
Corinne Cath	Article 19
Peter Ester	Eerste Kamerlid Christenunie
Bas Filippini	Privacy First
Valerie Frissen	SIDN Fonds
Arda Gerkens	Eerste Kamerlid SP
Hielke Hijmans	European Data Protection Supervisor
Mireille Hildebrandt	Vrije Universiteit Brussel
Jan Peter Loof	College voor de Rechten van de Mens
Ben van Lier	Centric
Franciose Rost	Rabobank
Cristiane Wopen	University of Cologne; scheidend voorzitter Deutscher Ethikrat

Rathenau Instituut

Daarnaast gaat er bijzondere dank uit naar de begeleidingscommissie van dit onderzoek die ons van waardevolle inzichten en advies heeft voorzien.

Naam	Organisatie
Dr. mr. Heleen Janssen	Min BZK, Constitutionele Zaken en Wetgeving
Dr. mr. Meine Henk Klijnsma	Min BZK, Constitutionele Zaken en Wetgeving
Prof. mr. Corien Prins	Tilburg University, Bestuurslid Rathenau Instituut
Prof. dr. Jeroen van den Hoven	Technische Universiteit Delft / 3TU
Prof. dr. Inez de Beaufort	Erasmus MC
Prof. dr. Victor Bekkers	Erasmus Universiteit

Rathenau Instituut

## Over de auteurs

Rinie van Est is themacoördinator bij het Rathenau Instituut. Hij is natuurkundige en politicoloog en signaleert nieuwe ontwikkelingen op het raakvlak van wetenschap, technologie, politiek en samenleving. Rinie houdt zich bezig met opkomende technologieën als nanotechnologie, biotechnologie, informatietechnologie en hersenwetenschappen. Hij houdt zich ook met het complexe energievraagstuk bezig. In 1999 promoveerde hij op het bestuurskundige proefschrift *Winds of Change*, over de interactie tussen politiek, technologie en economie op het gebied van windenergie in Californië en Denemarken. Rinie doceert ook aan de subfaculteit Technische Innovatie Wetenschappen van de TU Eindhoven. Recente publicaties waaraan hij heeft meegewerkt zijn *Rules for the digital human park* (2016), *Werken aan de robotsamenleving: Visies en inzichten uit de wetenschap over de relatie technologie en werkgelegenheid* (2015) en *Intieme technologie: De slag om ons lichaam en gedrag* (2014). In 2016 verscheen ook Engelstalige boek getiteld *Just ordinary robots: Automation from love to war*, dat werd gepubliceerd door Routledge.

Linda Kool is senior onderzoeker en projectleider bij het Rathenau Instituut. Ze houdt zich bezig met verschillende maatschappelijke vraagstukken op het gebied van digitale innovaties, zoals big data, internet of things, kunstmatige intelligentie, robotica en persuasieve technologie. Linda studeerde Sociale Wetenschappelijke Informatica aan de Universiteit van Amsterdam en heeft een Master in European Studies of Society, Science and Technology aan de Universiteit van Maastricht en Oslo. Voor het Rathenau Instituut, werkte Linda bij de onderzoeksorganisatie TNO waar ze keek naar vraagstukken rondom privacy en ICT. Ze is columnist voor het blad InGovernment. Recente publicaties waaraan zij heeft meegewerkt zijn: *Rules for the digital human park* (2016), *Beyond Control* (2016) over privacy en het Internet of Things, *Werken aan de robotsamenleving* (2015), *Dicht op de huid. Gezichts- en emotieherkenning in Nederland* (2015), *De datagedreven samenleving* (2015) en *Eerlijk advies. De opkomst van de e-coach* (2014).

Lambèr Royakkers is universitair hoofddocent ethiek van technologie bij de Technische Universiteit Eindhoven, afdeling Filosofie en Ethiek. Lambèr studeerde wiskunde en wijsbegeerte en maatschappijwetenschappen aan de TU Eindhoven en rechten aan de Universiteit van Tilburg. In 1996 promoveerde hij op een proefschrift over normenlogica. De laatste jaren houdt hij zich bezig met militaire ethiek, robotethiek, deontische logica en morele verantwoordelijkheid in onderzoeksnetwerken. Daarnaast is hij medeoprichter van het Landelijk Instituut voor Ethiektraining (LIVET). Hij is auteur en co-auteur van meer dan tien wetenschappelijke boeken, waaronder *Just ordinary robots: Automation from love to war* (2016), *Moral Responsibility and the Problem of Many Hands* (2015), *Ethics, Engineering and Technology* (2011).

Jelte Timmer is onderzoeker bij het Rathenau Instituut. In zijn werk kijkt hij naar de sociale en ethische impacts van digitale innovaties zoals sociale media, Internet of Things, gezichtsherkenningstechnologie, big data en persuasieve technologie. Hij studeerde sociale psychologie aan de Universiteit Utrecht, en heeft een Master in Kunstbeleid en Management en in Nieuwe Media en Digitale Cultuur. Voor hij bij het Rathenau Instituut begon, stond aan de start van het Utrechts centrum voor nieuwe media en digitale cultuur SETUP, waar hij nog als lid van de

Raad van Advies aan verbonden is. In de afgelopen jaren heeft hij verschillende essays, nieuwsartikelen en rapporten over digitale innovaties geschreven. Hij schreef bijvoorbeeld mee aan rapporten over de ethische kant van digitalisering voor de Raad van Europa (*From Bio to NBIC convergence, 2014*), de Global Summit of National Ethics Committees (*Rules for the digital human park, 2016*), en werkte aan het boek *Eerlijk Advies* (2014) over digitale gedragsbeïnvloeding. Andere recente publicaties zijn *Berekende risico's* (2015) en *Tem de robotauto* (2014). Hij is een veelgevraagd spreker en presenteerde zijn werk op internationale wetenschappelijke conferenties, bijeenkomsten voor het bedrijfsleven en populaire festivals zoals Lowlands.



### **Wie was Rathenau?**

Het Rathenau Instituut is genoemd naar professor dr. G.W. Rathenau (1911-1989). Rathenau was achtereenvolgens hoogleraar experimentele natuurkunde in Amsterdam, directeur van het natuurkundig laboratorium van Philips in Eindhoven en lid van de Wetenschappelijke Raad voor het Regeringsbeleid. Hij kreeg landelijke bekendheid als voorzitter van de commissie die in 1978 de maatschappelijke gevolgen van de opkomst van micro-elektronica moest onderzoeken. Een van de aanbevelingen in het rapport was de wens te komen tot een systematische bestudering van de maatschappelijke betekenis van technologie. De activiteiten van Rathenau hebben ertoe bijgedragen dat in 1986 de Nederlandse Organisatie voor Technologisch Aspectenonderzoek (NOTA) werd opgericht. NOTA is op 2 juni 1994 omgedoopt in Rathenau Instituut.

# **Rathenau Instituut**

Onderzoek & dialoog | Wetenschap, technologie en innovatie