Rathenau Instituut

Doelgericht digitaliseren

Hoe Nederland werkt aan een digitale transitie waarin mensen en waarden centraal staan

Rapport

Auteurs
Linda Kool, Elma Dujso en Rinie van Est

Redactie
Arnold Vonk

Foto omslag
Een bezoeker van het Rijksmuseum bekijkt Het Melkmeisje van Johannes Vermeer. Foto Rob Voss - Hollandse Hoogte

Bij voorkeur citeren als:
Kool, L., E. Dujso, en R. van Est (2018). *Doelgericht digitaliseren – Hoe Nederland werkt aan een digitale transitie waarin mensen en waarden centraal staan*. Den Haag: Rathenau Instituut

Voorwoord

Nog niet zo lang geleden waren algoritmen sommen voor wiskundigen, was *A.I.* een sciencefictionfilm en was *augmented reality* vooral leuk voor gamers. Ook de digitale samenleving was iets nieuws, dat velen optimistisch benaderden. Inmiddels is het besef gegroeid dat digitalisering een enorme kracht is die de samenleving snel verandert. Zo zet technologie voor gezichtsherkenning ons openbare leven op z'n kop en krijgt het *Internet of Things* een *boost* met de aanleg van 5G-netwerken.

In februari 2017 publiceerden we ons rapport *Opwaarderen*, na een verzoek van de Eerste Kamer aan het kabinet om uit te zoeken of de samenleving wel genoeg aandacht besteedde aan de ethische kant van digitalisering. De senatoren vermoedden van niet. Ons onderzoek liet inderdaad zien dat publieke waarden als privacy, veiligheid, gelijke behandeling en autonomie onder druk staan.

Anderhalf jaar later is dit nog steeds zo. Dit rapport is een overzicht van alle inspanningen op dit gebied tussen januari 2017 en juni 2018. We deden literatuuronderzoek en inventariseerden wat er in verschillende domeinen op ons af komt. Weliswaar werd het stelsel versterkt waarmee de samenleving zichzelf bestuurt – het 'governancesysteem'. Toch was de noodzaak niet eerder zo groot om digitalisering als transitie te zien, waarin waarden centraal staan en waarbij de samenleving niemand uitsluit. Overheid, bedrijven en burgers moeten daarom ook de komende jaren ieder hun verantwoordelijkheid nemen en samenwerken op lokaal, regionaal en internationaal niveau.

In juni gaf het kabinet een eerste aanzet met de Nationale Digitaliseringsstrategie. Daarin staan plannen om het governancesysteem te versterken op dit onderwerp. Het kabinet erkent dat het om een transitie gaat. Dat is winst.

We zien veel bewustwording en losstaande acties. Wat ontbreekt is de koppeling tussen maatschappelijke vraagstukken en innovatie. Voor een digitale transitie waarin mensen en waarden centraal staan, moeten overheden en bedrijven doelgerichter digitaliseren. Laten we zorgen dat alle partijen die meedoen aan de Digitale Top, die het kabinet in 2019 wil organiseren, meer doen dan alleen hun vorderingen presenteren. In dit rapport geven we daarom vijf aanbevelingen.

Dr. ir. Melanie Peters
Directeur Rathenau Instituut

Samenvatting

Nederland is het afgelopen anderhalf jaar gaan beseffen hoe groot de impact is van digitalisering op de samenleving. Digitalisering verwijst niet langer vooral naar een verzameling gadgets, maar blijkt een transitie te zijn met kansen en risico's. Het is dan ook de vraag voor de toekomst hoe Nederland die transitie moet vormgeven.

De belangrijkste boodschap van het Rathenau Instituut is dat de overheid, het bedrijfsleven en maatschappelijke organisaties de digitale samenleving zo moeten vorm- en richtinggeven dat mensen en waarden meer centraal komen te staan. Dan kan er een digitale samenleving ontstaan waarin niemand wordt uitgesloten. Daarom stellen we in dit rapport vijf acties voor.

Een vervolg op het rapport *Opwaarderen*
Dit rapport is een vervolg op ons rapport *Opwaarderen* uit februari 2017, dat we schreven naar aanleiding van de motie Gerkens die was aangenomen door de Eerste Kamer. Dat rapport bracht een breed spectrum aan maatschappelijke en ethische digitaliseringsvraagstukken in kaart.

We concludeerden in *Opwaarderen* dat digitalisering publieke waarden als privacy, digitale veiligheid, gelijke behandeling en vrijheid van meningsuiting onder druk zet. En dat het governancesysteem – het geheel aan actoren en instituties die maatschappelijke en ethische kwesties agenderen en vormgeven – onvoldoende was voorbereid om deze publieke waarden te beschermen. Daarom pleitten we voor versterking, oftewel, opwaardering, van het governancesysteem, en schreven we dat alle partijen daarvoor in actie moesten komen.

Het Rathenau Instituut vindt deze snelle update van het rapport *Opwaarderen* wenselijk, gezien de maatschappelijke relevantie en urgentie van het beschermen van publieke waarden in het digitale tijdperk.

Ethische vragen staan nadrukkelijker op de agenda
In dit rapport zien we dat de overheid, en vele andere partijen, de boodschap uit *Opwaarderen* hebben opgepakt. Diverse maatschappelijke en ethische vragen, bijvoorbeeld over inzicht in algoritmen of een eerlijke data-economie, staan veel nadrukkelijker op de agenda dan twee jaar geleden. Beleidsmakers, toezichthouders en maatschappelijke organisaties bouwen kennis op over deze nieuwe thema's. Op het gebied van privacy en veiligheid is de stap gemaakt van agenda- en beleidsvorming naar beleids*bepaling*. Het governancesysteem is in de afgelopen anderhalf jaar daarmee positief veranderd.

Op andere terreinen zijn thema's wel geagendeerd, maar nog niet vertaald naar concrete beleidsmaatregelen. Voorbeelden hiervan zijn de bescherming van de democratie, inzicht in algoritmen, en een eerlijke, competitieve data-economie.

Ook zijn sommige technologieën en daarmee samenhangende maatschappelijke kwesties nog niet geagendeerd. Voorbeelden hiervan zijn gezichtsherkenning, *virtual* en *augmented reality* en mogelijke gezondheidseffecten van digitale technologie.

Werken aan een digitale transitie die mensen en waarden centraal stelt
Vele partijen, zoals beleidsmakers, politici, maatschappelijke organisaties, regionale en lokale overheden, beroepsverenigingen en toezichthouders, voelen het belang van het beschermen van publieke waarden. Ze oriënteren zich op de vraag wat digitalisering betekent voor hun organisatie, sector of praktijk. De centrale vraag is hoe zij de digitale transitie in goede banen kunnen leiden. Velen erkennen dat bij digitalisering het beschermen van publieke waarden en grondrechten het uitgangspunt moet zijn.

Dit betekent een ommekeer in het debat over de inzet en de invloed van digitale technologieën: van een focus op technologie en de aanname dat dit vanzelf zal leiden tot maatschappelijke vooruitgang, naar een focus op de interactie tussen digitalisering en waarden. Digitalisering is daarbij enerzijds een middel om maatschappelijke uitdagingen aan te pakken, en anderzijds een ontwikkeling die publieke waarden onder druk kan zetten. Het transitieperspectief legt de vraag 'in welke digitale samenleving willen we leven', prominent op tafel. Om die vraag te kunnen beantwoorden, is een integrale innovatie-aanpak nodig, die vanuit publieke waarden vorm en richting geeft aan de digitale transitie en dus aan onze samenleving.

Vijf acties om het governancesysteem te versterken
Het Rathenau Instituut stelt vijf acties voor waarmee beleidsmakers, bedrijven, en maatschappelijke organisaties het governancesysteem kunnen versterken:

1. **Investeer in een waardengedreven benadering van innovatie**
   Ethische en maatschappelijke vraagstukken staan niet los van innovatie- of digitaliseringsprocessen. Om de ambities van Nederland waar te kunnen maken, bijvoorbeeld in de zorg, in de energietransitie of op het gebied van mobiliteit, is het van belang innovatie te verbinden aan maatschappelijke vraagstukken: Nederland moet publieke waarden niet zien als sluitstuk van innovatie, maar als uitgangspunt daarvan. Dit sluit aan bij het denken over innovatiebeleid in termen van missiegedreven innovatiebeleid of doelgerichte innovatiesystemen.

2. **Kom tot een proactieve, overkoepelende agenda en activiteitenplan voor maatschappelijke en ethische aspecten van digitalisering**
   Maatschappelijke en ethische digitaliseringsvraagstukken zijn op de beleidsagenda gekomen. Maar er is nog geen integraal beeld. Diverse kwesties zijn nog niet vertaald naar concrete beleidsmaatregelen. Een proactieve agenda vraagt ook om aandacht voor thema's die nog nauwelijks op de agenda staan, zoals gezichtsherkenning, *virtual* en *augmented reality* en mogelijke gezondheidseffecten van technologieën. Een overkoepelende agenda bevat ook een visie op hoe de samenleving te betrekken (zie punt 5).

3. **Investeer in een sterke positie van toezichthouders**
   Toezichthouders vormen een cruciale schakel in de versterking van het governancesysteem op het gebied van digitaliseringskwesties. Zij hebben daar ook meer aandacht voor. Ze investeren in kennisopbouw en in samenwerking met andere toezichthouders. Diverse toezichthouders kregen nieuwe bevoegdheden, of meer budget. Het is belangrijk om te monitoren of, en in hoeverre dat toereikend is. De acties om toezichthouders te versterken kunnen we zien als eerste stappen. We beginnen net te begrijpen waartoe digitalisering in staat is. Het is daarom vanuit strategisch oogpunt van belang te blijven investeren in de mogelijkheden en capaciteiten van toezichthouders.

4. **Bedrijfsleven: maak werk van maatschappelijk verantwoord digitaliseren**
   De politiek en de samenleving zijn zich steeds meer bewust van de maatschappelijke en ethische vraagstukken op het gebied van digitalisering. Dat leidt tot toenemende druk op het bedrijfsleven om deze serieus op te pakken. Maatschappelijk verantwoord ondernemen op het vlak van digitalisering vraagt om een proactieve houding van het bedrijfsleven, om maatschappelijke en ethische implicaties van een technologie die een bedrijf ontwikkelt te voorzien en daarop te anticiperen. Bedrijven zijn op diverse manieren verplicht om zich in te spannen om mensenrechten te beschermen. Ze zijn nu aan zet om deze zorgplichten vorm te geven in de praktijk.

5. **Stimuleer technologisch burgerschap**
   Om richting te kunnen geven aan innovatie, moeten burgers daarbij betrokken zijn. Daarom moeten ze weten wat de mogelijkheden en risico's van technologie zijn, en moeten ze kunnen deelnemen aan het democratisch debat en aan politieke besluitvorming. Het blijven stimuleren van deze drie elementen is essentieel voor een sterk governancesysteem. Daarbij moet er aandacht zijn voor de grenzen van de zelfredzaamheid van burgers, en voor hun bereidheid om te participeren. Waardengedreven innoveren betekent innovatie vormgeven vanuit gedeelde, publieke waarden. Dat kan alleen in gesprek met de samenleving. Daarvoor is een visie van de overheid nodig.

Inhoud

Voorwoord 3

Samenvatting 4

Inleiding 9
1.1 Achtergrond 9
1.2 Doel van dit rapport 11
1.3 Digitalisering en publieke waarden 12
1.4 Governancesysteem 15
1.5 Onderzoeksopzet en -methode 19
1.6 Leeswijzer 21

2 Grond- en mensenrechten 22
2.1 Nederland 22
2.2 Raad van Europa 24
2.3 Internationaal 28
2.4 Conclusie 31

3 Maatschappelijke actoren en debat 33
3.1 Hoofdpunten uit het debat in de media 34
3.1.1 Nederland 34
3.1.2 Internationaal 36
3.2 Maatschappelijke organisaties 37
3.3 Koepelorganisaties bedrijfsleven en werknemers 44
3.4 Internationale ontwikkelingen 47
3.5 Conclusie 49

4 Politiek en bestuur: agendavorming 51
4.1 Nederland 51
4.2 Internationale ontwikkelingen 66
4.3 Conclusie 70

5 Politiek en bestuur: beleidsvorming en -bepaling 72
5.1 Kabinet en ministeries 73
5.1.1 Ministerie van BZK 73
5.1.2 Ministerie van EZK 77
5.1.3 Ministerie van JenV 82
5.1.4 Ministerie van OCW 86

5.1.5 Ministerie van BuZa 88
5.2 Eerste en Tweede Kamer 89
5.3 Europese Commissie 92
5.4 Europees Parlement 97
5.5 Conclusie 101

6 Politiek en bestuur: toezichthouders 103
6.1 Nederland 103
6.2 Internationaal 114
6.3 Conclusie 116

7 Vanuit publieke waarden vormgeven aan digitale transitie 117
7.1 Digitale transitie 117
7.2 Opwaarderen is van start gegaan 118
7.2.1 Stand van zaken medio 2018 119
7.2.2 Verbreding van het debat 123
7.3 Blinde vlekken ten dele ingevuld 124
7.4 Aanbevelingen 131
7.5 Tot slot 136

Literatuurlijst 137

Bijlage 1 Kamervragen en moties 151

Bijlage 2 De betekenis van publieke governance 160

Inleiding

1.1 Achtergrond

In de motie Gerkens c.s. van 23 september 2014 riep de Eerste Kamer de regering op '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). Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties gaf gehoor aan deze oproep en vroeg ons eind 2015 dit onderzoek te gaan doen.

Daarop publiceerden wij op 9 februari 2017 het rapport *Opwaarderen. Borgen van publieke waarden in de digitale samenleving* (Kool et al. 2017).[1] Hierin brachten wij in kaart hoe het 'governancesysteem' eruitziet op het gebied van ethische en maatschappelijke kwesties rondom digitalisering: het geheel aan actoren en instituties dat maatschappelijke en ethische vraagstukken agendeert en vormgeeft.

Governance betreft kort gezegd het collectief besturen van maatschappelijke problemen in onze samenleving. Het draait om vragen als:

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

We keken naar acht centrale technologische digitaliseringstrends (zie ook tabel 1):

1. robotica;
2. het Internet of Things (IoT);
3. biometrie;
4. persuasieve technologie;
5. digitale platformen (inclusief blockchain);
6. *virtual* en *augmented reality* en sociale media;
7. *big data* en algoritmen; en
8. kunstmatige intelligentie (AI).

We lieten zien dat deze trends tal van maatschappelijke en ethische vragen met zich meebrengen. Naast bekende IT-gerelateerde maatschappelijke thema's, zoals privacy en veiligheid, gaat het daarbij om – voor het IT-domein opkomende –

1 Zie ook: https://www.rathenau.nl/nl/digitale-samenleving/opwaarderen

thema's, zoals autonomie, rechtvaardigheid, menselijke waardigheid, controle over technologie, en machtsverhoudingen. De verbreding van de maatschappelijke en ethische kwesties rondom digitalisering hangt samen met de 'cybernetische feedback-loop': het feit dat data op grote schaal worden verzameld, en inmiddels ook op grote schaal worden geanalyseerd en toegepast (zie figuur 1). Met andere woorden: digitalisering wordt steeds meer 'cybernetisering'.

In de studie *Opwaarderen* lieten we zien dat het er begin 2017 slecht voor staat met het Nederlandse governancesysteem op het gebied van de (opkomende) maatschappelijke en ethische thema's die samenhangen met digitalisering. We identificeerden vijf blinde vlekken die op korte termijn geadresseerd moesten worden. Het ging niet goed met:

1. de vertaling van nieuwe maatschappelijke en ethische vraagstukken naar beleid; het ontbrak aan interdepartementale afstemming en coördinatie op digitalisering en aan politiek debat over die nieuwe vraagstukken;
2. de borging van grond- en mensenrechten in de digitale samenleving;
3. het versterken van toezichthouders en zorgen voor onderlinge afstemming tussen toezichthouders;
4. de nieuwe verantwoordelijkheden voor ontwikkelaars van digitale diensten en producten; en
5. het organiseren van maatschappelijk tegengeluid – met het versterken van het maatschappelijk middenveld, de kennis en vaardigheden van burgers en het maatschappelijk debat over digitalisering.

Het rapport *Opwaarderen* liet daarmee zien dat publieke waarden in onze digitale samenleving onvoldoende werden beschermd. We concludeerden dat het governancesysteem versterkt moet worden. De belangrijkste boodschap was dan ook dat 'de overheid, het bedrijfsleven en het maatschappelijke middenveld nu actie dienen te ondernemen om het governancelandschap te versterken en zo publieke waarden in de digitale samenleving te kunnen blijven borgen' (Kool et al. 2017, 12). Daarbij stelden we vijf acties voor aan de genoemde partijen:

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.

1.2 Doel van dit rapport

Het rapport *Opwaarderen* was zodoende een *wake-up call*, die de overheid, het bedrijfsleven en maatschappelijke organisaties wakker wilde schudden. Het zette aan tot meer aandacht en actie met betrekking tot het waarborgen van publieke waarden op het terrein van digitalisering. Het rapport dat voor u ligt betreft een actualisering van *Opwaarderen.*

Waarom volgt deze update al zo snel? Ten eerste heeft dit te maken met de door het Rathenau Instituut gevoelde grote urgentie van het waarborgen van publieke waarden in onze digitale samenleving. Twee werkconferenties die het Rathenau Instituut in samenwerking met de Sociaal-Economische Raad (SER) heeft georganiseerd, lieten zien dat deze gevoelde relevantie en urgentie ook door tal van maatschappelijke stakeholders ervaren worden.[2] Ook binnen de Eerste en Tweede Kamer wordt het gevoel van urgentie door vele partijen gedeeld.

Ten tweede zijn er de afgelopen twee jaar op het gebied van de governance van maatschappelijke en ethische digitaliseringsvraagstukken tal van activiteiten ontplooid. Het gewenste proces van opwaarderen van het governancesysteem lijkt zodoende van start te zijn gegaan.

Dit onderzoek wil laten zien welke initiatieven er op diverse terreinen zijn genomen. We proberen een integraal beeld te schetsen van de wijze waarop de afgelopen twee jaar stappen zijn gezet met betrekking tot het opwaarderen en bij de tijd brengen van het Nederlandse governancesysteem op het terrein van ethische en maatschappelijke kwesties van digitalisering. Het doel van deze studie is via deze update bij te dragen aan de verdere versterking en modernisering van het governancesysteem, en daarmee aan het adequaat waarborgen van publieke waarden in onze digitale samenleving.

Dat doel is nog lang niet bereikt. Een breed overzicht van de huidige stand van zaken van het governancesysteem kan inzicht bieden in hoe de modernisering daarvan op een goede en effectieve manier verder vormgegeven kan worden.

2 Zie Rathenau Instituut & SER (2018). *Acties voor een verantwoorde digitale samenleving*. Het doel hiervan was te verkennen welke kwesties rondom digitalisering maatschappelijke actoren als urgent beschouwen, en welke mogelijkheden maatschappelijke actoren zien voor eventuele oplossingen en acties op dit vlak. Deelnemers waren onder meer bedrijven, kennisorganisaties, belangenorganisaties van consumenten of burgers, de nationale overheid, uitvoeringsorganisaties, toezichthouders en lokale overheden. Zie ook: https://www.rathenau.nl/nl/digitale-samenleving/acties-voor-een-verantwoorde-digitale-samenleving

1.3 Digitalisering en publieke waarden

Digitalisering biedt de maatschappij volop economische en maatschappelijke kansen. Zoals efficiënter zakendoen, eerder ziektes opsporen of sneller kennis delen. Als we in dit rapport spreken over ‘digitalisering’, doelen we op een cluster van digitale technologieën die nu en in de komende jaren een plek zullen krijgen in onze samenleving. Dit cluster bestaat uit acht technologiegebieden, weergegeven in tabel 1 (zie ook Kool et al. 2017).

Tabel 1 Overzicht technologiegebieden

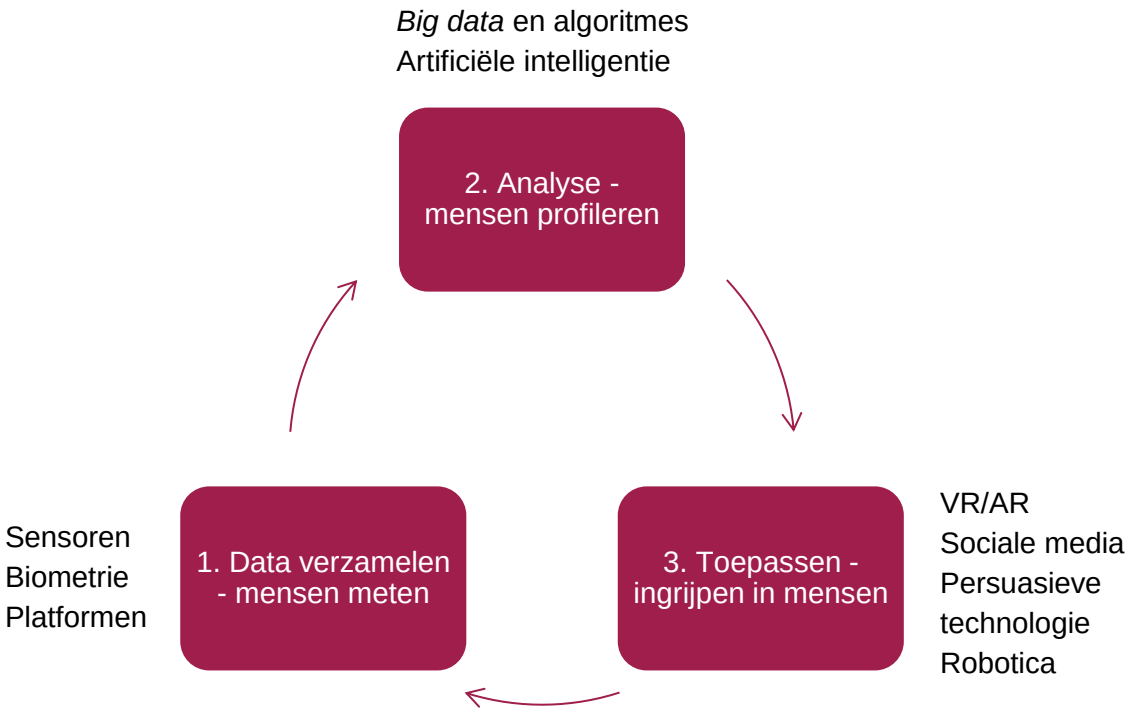
Overzicht technologiegebieden
Robotica
Internet of Things (IoT)
Biometrie
Persuasieve technologie
Digitale platformen (incl blockchain)
Virtual en *augmented reality*
Big data en algoritmen
Kunstmatige intelligentie (AI)

Bron: Rathenau Instituut

Door deze technologieën raken steeds meer aspecten uit de fysieke wereld verbonden met de digitale wereld. Er ontstaat een cybernetische feedback-loop waarin data wordt verzameld, geanalyseerd en direct wordt toegepast. Of, in andere woorden, een feedback-loop van het meten van mensen, het profileren van mensen, en het ingrijpen in mensen, hun gedrag of hun omgeving (zie figuur 1).

De bovengenoemde technologiegebieden spelen in verschillende onderdelen van deze feedback-loop een rol (zie figuur 1). Mensen profileren gebeurt bijvoorbeeld vaak aan de hand van *big data* en algoritmen, en kunstmatige intelligentie (AI). Maar deze technologieën incorporeren vaak meerdere elementen van deze loop. Een sociaal netwerk, zoals Facebook, verzamelt niet alleen data, maar analyseert deze data om het platform aan te passen.

Figuur 1 Cybernetische feedback-loop



Bron: Rathenau Instituut

In het rapport *Opwaarderen* stellen we dat hoewel digitalisering al decennia aan de gang is, we door deze feedback-loop een nieuwe fase in de digitale samenleving inluiden. De feedback-loop maakt namelijk ‘real-time’ bijsturen in de fysieke wereld mogelijk.

Dit is bijvoorbeeld zichtbaar in slimme leerplatformen, die prestaties van leerlingen volgen, en hen op basis daarvan passende leeropdrachten aanbieden. Het kan een slimme thermostaat zijn, die op basis van informatie over het huis en analyse van het gedrag van de bewoners, automatisch de temperatuur in huis regelt. Of een slimme lantaarnpaal op straat, die met behulp van sensoren gedrag van mensen meet, en via licht het gedrag tracht te beïnvloeden.

Het kunnen ‘sluiten’ van de feedback-loop – het ‘real-time’ bijsturen in de fysieke wereld – roept nieuwe ethische en maatschappelijke vragen op. Op basis van wetenschappelijke literatuur identificeerden we in *Opwaarderen* zeven ethische en maatschappelijke thema’s, die ook in dit rapport centraal zullen staan; zie tabel 2. De thema’s zijn te zien als belangrijke publieke waarden, die nauw verwant zijn aan grond- en mensenrechten. Kwesties als 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 en de Universele Verklaring van de Rechten van de Mens. Waarden zoals autonomie, gelijke machtsverhoudingen en controle over technologie worden niet expliciet benoemd in verdragen, maar kunnen gezien worden als onderdeel van of volgend uit deze grond- en mensenrechten.

Tabel 2 Overzicht maatschappelijke en ethische thema's[3]

Thema	Vraagstuk
Privacy	Gegevensbescherming, 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, de-skilling, de-socialisatie, werkloosheid
Rechtvaardigheid	Discriminatie, uitsluiting, gelijke behandeling, stigmatisering
Machtsverhoudingen	Oneerlijke concurrentie, uitbuiting, relatie consument-bedrijf

Bron: Rathenau Instituut

De processen in de feedback-loop van data roepen verschillende maatschappelijke en ethische kwesties op, zoals weergegeven in figuur 2. Het proces van dataverzameling en verwerking (het meten) leidt vooral tot discussies over privacybescherming. De telkens toenemende mogelijkheden om persoonlijke gegevens te verzamelen bedreigen nieuwe dimensies van privacy.

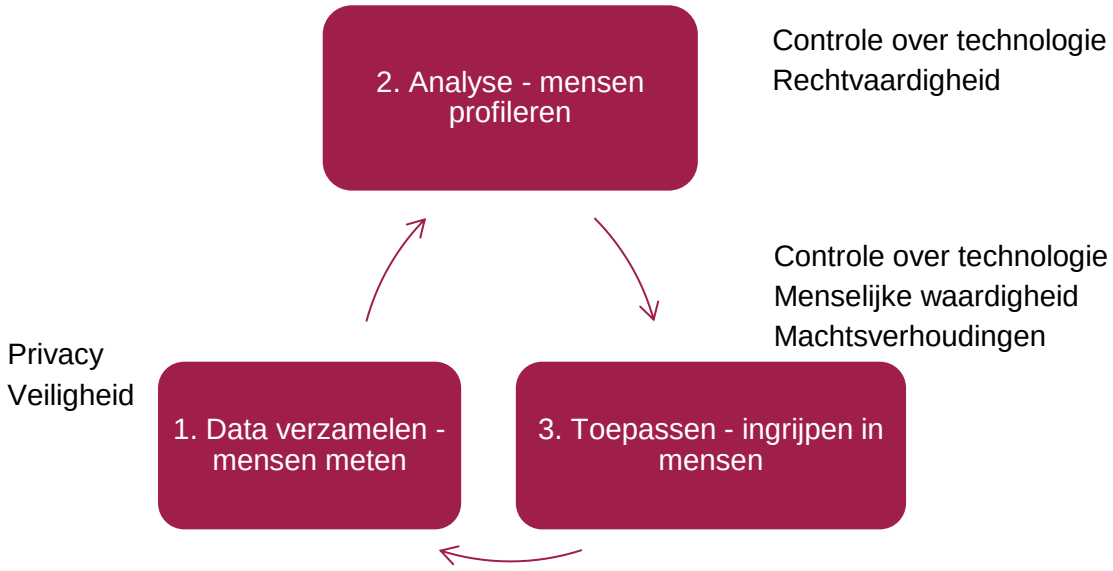
- Zo leidt de vooruitgang in technieken als gezichts- en emotieherkenning tot discussies over de vrijheid om te denken en voelen wat je wilt ('mentale privacy').
- Het proces van data-analyse (het profileren) en de nieuwe technieken die daarvoor worden ingezet (zoals zelflerende algoritmen) leiden tot zorgen over het recht op gelijke behandeling en menselijke waardigheid (en over de rol van mensen ten opzichte van computers en andere machines).

3 Deze thema's zijn tot stand gekomen door een uitgebreide literatuuranalyse. Per technologiegebied is gezocht naar wetenschappelijke literatuur naar maatschappelijke en ethische aspecten in de periode 2010-2016. De gevonden maatschappelijke en ethische kwesties zijn geclusterd in deze 7 thema's.

- 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.

In dit rapport gebruiken we figuur 2 om te verduidelijken hoe de discussie over maatschappelijke en ethische kwesties rondom digitalisering zich ontwikkelt. Welke technologiegebieden en thema's staan op de agenda, en op welke manier?

Figuur 2 Cybernetische feedback-loop en bijbehorende maatschappelijke en ethische kwesties



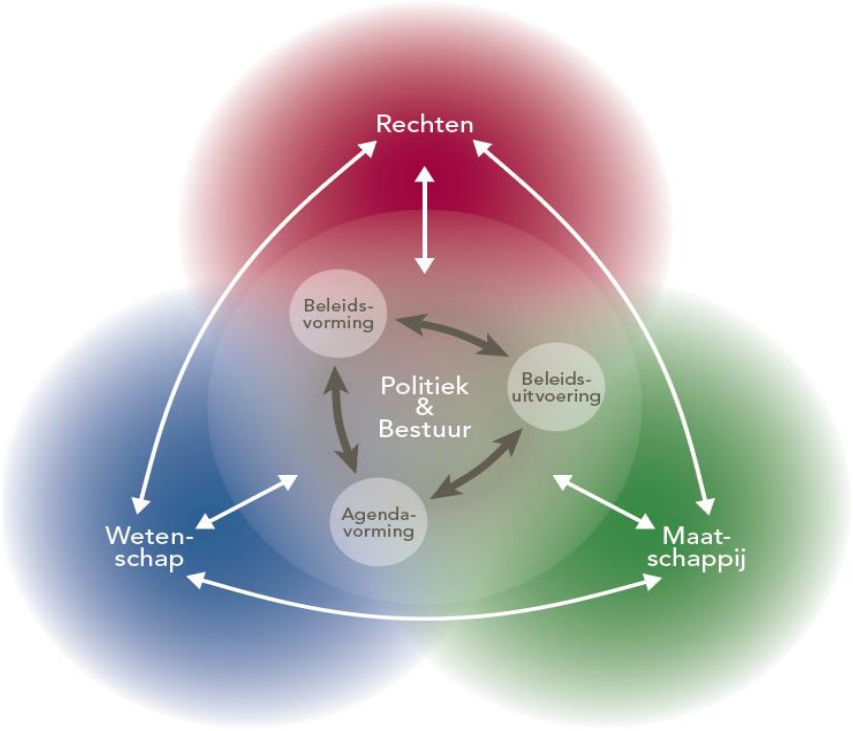
Bron: Rathenau Instituut

1.4 Governancesysteem

In dit rapport staat de governance van ethische en maatschappelijke uitdagingen rond digitalisering centraal. We maken hierbij gebruik van het conceptuele raamwerk uit *Opwaarderen*. Van belang voor onze aanpak is het onderscheid dat we maken tussen governance en meta-governance (zie bijlage 2).[4]

4 Deze hele paragraaf 1.4 is gebaseerd op paragraaf 4.8 ('Raamwerk voor het governance-ecosysteem') in *Opwaarderen*. Bijlage 2 is vrijwel gelijk aan Appendix B uit dat rapport.

Figuur 3 Het governancesysteem



Bron: Rathenau Instituut

Governance betreft zoals gezegd het collectief aanpakken van maatschappelijke problemen in onze samenleving.[5] Het draait om vragen als:

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

Meta-governance geeft aan dat het collectieve bestuur van maatschappelijke problemen plaatsvindt in een governancesysteem, 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 maatschappelijke 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?

5 Governance is gericht op het aanpakken van publieke vraagstukken. Het gaat om maatschappelijke problemen, oftewel problemen die slechts via collectieve actie opgelost kunnen worden (vgl. Hoppe 2010).

In dit rapport kijken we vooral naar het **governancesysteem** op het gebied van maatschappelijke en ethische kwesties rondom digitalisering. Dit ontwikkelden we in *Opwaarderen*.[6] We onderscheiden in dit raamwerk vier domeinen; zie figuur 3: 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.

Grond- en mensenrechten

Ethische en maatschappelijke discussies rond nieuwe technologie draaien vaak om de vraag welke waarden in het geding zijn. Daarbij wordt vaak verwezen naar grond- en mensenrechten. Mensenrechten zijn rechten die ieder mens toekomen. Ze moeten mensen beschermen tegen de macht van de staat en ze moeten ervoor zorgen dat iedereen kan leven in menselijke waardigheid.[7] Ze zijn onder meer 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
- 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 ook onder druk zetten. Ze kunnen ook aanleiding zijn om bestaande mensen- of grondrechten te herformuleren, of om nieuwe mensen- of grondrechten op te nemen. In dit rapport bekijken we in dit domein de activiteiten van instanties die kijken naar de betekenis van nieuwe technologieën voor mensen- en grondrechten, zoals Staatscommissies, de Raad van Europa, of de VN-Mensenrechtenraad.

Maatschappij

Maatschappelijke actoren, zoals bedrijven, non-gouvernementele organisaties (ngo’s) en burgers, spelen een belangrijke rol in de governance van maatschappelijke en ethische vragen rondom digitalisering:

6 We deden dit door een historisch overzicht te geven voor de omgang met maatschappelijke en ethische kwesties op het gebied van vier technologieën: ICT, biotechnologie, gentechnologie en dierexperimenten.

7 Zie de website van het College voor de Rechten van de Mens: http://www.mensenrechten.nl/wat-zijn-mensenrechten/wat-zijn-mensenrechten

- 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 ethische en maatschappelijke digitaliseringsvraagstukken, en dragen bij aan bewustwording van individu.
- En ieder individu geeft met zijn eigen keuzes en handelen uiteraard ook vorm aan hoe digitale technologie een plek krijgt in de maatschappij.

Wetenschap
Wetenschappelijke kennis kan behulpzaam zijn bij
- zowel de signalering als articulatie van maatschappelijke en ethische aspecten,
- het formuleren van een beleidsopvatting en bepalen van een handelingsperspectief (beleidsvorming); en
- bij reflectie op de uitvoering van beleid.

De wetenschap draagt direct bij aan 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 of Eerste Kamer. Nationale adviesraden en publieke kennisorganisaties leveren ook kennis voor beleid.

In *Opwaarderen* brachten we in kaart welke maatschappelijke en ethische kwesties wetenschappers op het gebied van digitalisering signaleerden. We vatten ze samen in zeven publieke waarden, en we gebruiken deze wetenschappelijke analyse in dit rapport, om aan te geven welke kwesties wel en niet besproken worden.

Politiek en bestuur: agendavorming
Bij agendavorming kijken we in deze studie naar de professionele adviesorganen, 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 bij het vormen van de beleidsagenda. Deze fase wordt ook wel ‘ethische deliberatie’ genoemd (Ladikas et al. 2015).

Politiek en bestuur: beleidsvorming en -bepaling
Deliberatie over ethische en maatschappelijke vraagstukken kan leiden tot beleidsvorming en -bepaling: een fase waarin (politieke) besluiten over de gesignaleerde kwesties worden voorbereid en genomen. In een democratische samenleving zijn er altijd verschillen van inzicht, mening en levensovertuiging over

hoe om te gaan met maatschappelijk ethische vragen. Daarom is in de politieke besluitvorming een speciale rol weggelegd voor het parlement.

De fase van beleidsvorming en -bepaling kan leiden tot het opstellen of aanpassen van regelgevende kaders en tot beslissingen over beleidsinstrumenten, zoals het instellen van een trendanalyse, het instellen van een tijdelijke commissie, het opzetten van een maatschappelijke dialoog of het verstrekken van onderzoeksfinanciering.

Politiek en bestuur: 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.

1.5 Onderzoeksopzet en -methode

Samengevat, actualiseren we in dit rapport het governancesysteem van ethische en maatschappelijke digitaliseringsvraagstukken. We zullen de volgende vragen beantwoorden: Welke acties hebben diverse actoren sinds 2017 ondernomen om ethische en maatschappelijke vragen omtrent digitalisering aan te kaarten, of om te zetten in beleid? Wat is er veranderd sinds *Opwaarderen*?

In deze studie willen we vooral een overzicht geven van de kwesties en waarden die partijen politiek agenderen, en welke kwesties en waarden niet, en welke partijen en instituties er zijn om deze kwesties politiek aan te kaarten. We geven geen inhoudelijke beoordeling van de acties en initiatieven van actoren.

Om te kijken welke kwesties en digitale technologiëen worden geagendeerd, maken we gebruik van de acht geselecteerde technologiegebieden in *Opwaarderen* (tabel 1) en de zeven ethische en maatschappelijke thema's (tabel 2).

Op basis van *deskresearch* brengen we in kaart welke partijen welke kwesties agenderen, en hoe politiek en beleidsmatig wordt omgegaan met de gesignaleerde problemen. De beschrijvingen van de adviesraden, toezichthouders en belangenorganisaties zijn tot stand gekomen op basis van *deskresearch* en contact met desbetreffende organisaties. In ieder hoofdstuk behandelen we een van de vier domeinen uit het governancesysteem (grond- en mensenrechten, maatschappij,

agendavorming, beleidsvorming en –bepaling en beleidsuitvoering; zie figuur 3). Per domein bespreken we de relevante actoren. De focus ligt op ontwikkelingen in Nederland, maar we noemen ook enkele relevante ontwikkelingen in Europa. De onderzochte periode is 1 januari 2017 en 30 juni 2018. De uitzondering is de Digitale Agenda Overheid, die in juli 2018 uitkwam, maar gezien het belang voor dit onderwerp, wel mee is genomen. In tabellen vatten we de activiteiten samen.[8]

Bij maatschappelijke actoren (hoofdstuk 3) benoemen we belangrijke onderwerpen in de media. Ook brengen we de activiteiten van diverse belangenverenigingen van burgers, consumenten, professionals en het bedrijfsleven (waaronder werkgevers- en werknemersorganisaties) in kaart. En we benoemen enkele Europese en internationale maatschappelijke organisaties en belangenverenigingen. Door deze organisaties aangespannen rechtszaken behandelen we ook bij maatschappelijke actoren. We kijken niet naar organisaties uit afzonderlijke Europese landen. Ook individuele bedrijven laten we buiten beschouwing.

Bij agendavorming (hoofdstuk 4) kijken we bij de adviesraden naar de rapporten die in deze periode zijn gepubliceerd. Essays en rondetafelgesprekken en andere activiteiten van de adviesraden zijn buiten beschouwing gelaten. De kabinetsreacties op de rapporten van de adviesraden horen volgens het raamwerk bij beleidsvorming (hoofdstuk 5), maar worden omwille van de leesbaarheid in samenhang met de rapporten bij agendavorming besproken. Bij beleidsvorming verwijzen we uiteraard terug naar deze kabinetsreacties. Het Rathenau Instituut is onderdeel van het governancesysteem rondom maatschappelijke en ethische kwesties van technologie en van digitalisering. Het Rathenau Instituut heeft als expliciete taak publieke en politieke meningsvorming over wetenschap en technologie te stimuleren. In hoofdstuk 4 benoemen we daarom ook de activiteiten van het Rathenau Instituut.

Bij beleidsvorming en -bepaling (hoofdstuk 5) richten we ons op de beleidsactiviteiten van ministeries die het meest van doen hebben met ethische en maatschappelijke aspecten van de digitale samenleving. Dat zijn de ministeries van Binnenlandse Zaken en Koninkrijksrelaties (BZK), Economische Zaken en Klimaat (EZK), Justitie en Veiligheid (JenV), Onderwijs, Cultuur en Wetenschap (OCW) en Buitenlandse Zaken (BuZa).[9] We kijken naar de meest relevante documenten, zoals agenda's, strategieën of nota's over maatschappelijke en ethische aspecten van digitalisering. We kijken ook naar de activiteiten van de Eerste en Tweede Kamer. We kijken voor de periode 1 januari 2017 - 30 juni 2018 naar schriftelijke vragen en ingediende moties over maatschappelijke en ethische digitaliseringskwesties, en

8 We danken Tim Jacquemard voor de dataverwerking.

9 Daarmee is niet gezegd dat andere ministeries, op deelgebieden, niet met ethische en maatschappelijke aspecten van digitalisering in aanraking komen.

naar gehouden deskundigenbijeenkomsten (Eerste Kamer) en rondetafelgesprekken (Tweede Kamer) (zie Bijlage 1). In dit hoofdstuk benoemen we ook enkele beleidsinitiatieven van de Europese Commissie (op het vlak van de digitale eengemaakte markt) en van het Europees Parlement (resoluties die betrekking hebben op maatschappelijke en ethische aspecten van digitalisering).

Sommige actoren (koepelorganisaties, ngo's, adviesraden en dergelijke) komen niet terug in de analyse, indien zij geen rapporten/activiteiten hebben ondernomen in de onderzochte periode op het terrein van ethische en maatschappelijke vraagstukken in de digitale samenleving. Actoren, rapporten of beleidsstukken die wel aandacht besteden aan digitalisering, maar bijvoorbeeld vooral naar de financieel-economische of technische kant kijken, laten we buiten beschouwing. Desondanks kan ons overzicht niet compleet zijn, gezien het grote aantal relevante initiatieven dat in de onderzochte periode is ontplooid.

Dit onderzoek volgt de richtlijnen van het kwaliteitsbeleid van het Rathenau Instituut. Daarnaast is er een interne review geweest door een onderzoeker die niet betrokken was bij het onderzoek.

1.6 Leeswijzer

Dit rapport is als volgt opgebouwd:

- Hoofdstuk 2, **Grond- en mensenrechten**, geeft een overzicht van de activiteiten van de instituties die zich bezighouden met grond- en mensenrechten rondom digitalisering en publieke waarden, zoals staatscommissies, en in Europa de Raad van Europa.
- Hoofdstuk 3, **Maatschappelijke actoren**, brengt de activiteiten in kaart van diverse maatschappelijke actoren en de media als het gaat om publieke waarden en digitalisering. We bespreken diverse belangenorganisaties voor consumenten, werkgevers en werknemers.
- Hoofdstuk 4, **Agendavorming**, toont de publicaties van diverse adviesraden in Nederland en Europa op het vlak van digitalisering en publieke waarden.
- Hoofdstuk 5, **Beleidsvorming en -bepaling**, geeft de activiteiten van diverse ministeries weer en van het Nederlandse parlement. Daarnaast benoemen we relevante beleidsinitiatieven van de Europese Commissies en enkele relevante initiatieven in het buitenland.
- Hoofdstuk 6, **Beleidsuitvoering**, biedt een overzicht van de activiteiten van toezichthouders en andere controlerende instanties op het vlak van publieke waarden en digitalisering.
- Hoofdstuk 7, **Conclusies**, vat de bevindingen samen en geeft de conclusies weer.

2 Grond- en mensenrechten

In dit hoofdstuk beschrijven we de activiteiten van instituties die zich richten op digitalisering en de betekenis daarvan voor grond- en mensenrechten. We kijken naar Nederland (zoals staatscommissies), de Raad van Europa en naar de Verenigde Naties (VN).

Ten opzichte van het rapport *Opwaarderen* zien we de aandacht voor diverse technologiegebieden en de betekenis voor grond- en mensenrechten toenemen, zoals *big data*, AI, persuasieve technologie, platformen en robotica. Daarmee zijn ook andere kwesties dan alleen privacy op de beleidsagenda gekomen. Instituties als de Raad van Europa en de VN vragen nu ook aandacht voor vrijheidsrechten (zoals vrijheid van meningsuiting en vrijheid van associatie), gelijkheidsrechten, het recht op een eerlijk proces in relatie tot digitalisering.

Het valt op dat er nog weinig aandacht is voor technologiegebieden als biometrie (gezichtsherkenning) en *virtual* en *augmented reality* en de betekenis voor grond- en mensenrechten.

2.1 Nederland

Privacy
In Nederland loopt al geruime tijd een discussie of, en in hoeverre, de Nederlandse Grondwet aangepast dient te worden aan het digitale tijdperk. In 2009 werd de Staatscommissie Thomassen ingesteld om, mede in het licht van digitalisering, te adviseren over een mogelijke herziening van de Nederlandse grondrechten. In 2010 adviseerde de staatscommissie om de grondrechten aan te passen in lijn met de ontwikkelingen in de informatietechnologie.

Specifiek stelde de commissie voor om artikel 13 van de Grondwet te wijzigen. Artikel 13 betreft de onschendbaarheid van het brief-, telefoon-, en telegraafgeheim. De commissie stelde voor de reikwijdte van artikel 13 uit te breiden naar alle communicatiemiddelen, om zo te komen tot een techniekonafhankelijke bescherming (Kamerstukken II 2010-2011, 31570, nr 20). Op 11 juli 2017 heeft de Eerste Kamer de voorgestelde grondwetswijziging

aangenomen.[10][11] Daarmee is het voorstel in eerste lezing door beide Kamers. In 2018 en 2019 volgt de tweede lezing in respectievelijk de Tweede Kamer en de Eerste Kamer (deze is noodzakelijk voor een grondwetswijziging).

Algoritmen en grondrechten

Nieuw op de beleidsagenda in Nederland is de aandacht voor de betekenis van algoritmen voor andere grondrechten dan privacy. Het ministerie van Binnenlandse Zaken en Koninkrijkrelaties (BZK) verkent de betekenis van algoritmen, *big data* en AI op grondrechten (zie ook hoofdstuk 5). Specifiek gaat het om (Vetzo et al. 2018):

- privacyrechten (waaronder menselijke waardigheid, persoonlijke autonomie en zelfbeschikking);
- gelijkheidsrechten (recht op non-discriminatie);
- vrijheidsrechten (waaronder vrijheid van meningsuiting, godsdienstvrijheid, vrijheid van vereniging en het kiesrecht); en
- procedurele rechten (recht op een eerlijk proces).

Het kabinet verwacht in het najaar van 2018 zijn reactie op dit onderzoek aan de Tweede Kamer te sturen.

Digitalisering en bescherming democratie

De betekenis van digitalisering voor het democratische stelsel – met name op het vlak van *big data*, algoritmen en *microtargeting* (het zo veel mogelijk personaliseren van politieke boodschappen) – is ook nieuw op de beleidsagenda gekomen. Begin 2017 is de ‘Staatscommissie parlementair stelsel’ ingesteld. Die moet onderzoeken of het Nederlandse parlementaire stelsel nog goed werkt, en of dit toekomstbestendig is.[12] De staatscommissie onderzoekt ook de invloed van digitalisering op de (toekomstige) werking van het parlementair stelsel.

Volgens de commissie zorgen het gebruik van *big data* en *microtargeting* in verkiezingscampagnes en de mogelijkheid dat democratische instituties worden gehackt ervoor, dat fundamentele democratische waarden in het geding kunnen komen (Staatscommissie parlementair stelsel, 2017, p. 57). De staatscommissie zal eind 2018 haar advies uitbrengen. Daarnaast heeft het ministerie van BZK de Raad voor het Openbaar Bestuur gevraagd onderzoek te doen naar de effecten van

10 Op 19 augustus 2017 is de officiële verklaring afgelegd voor de verandering van artikel 13 van de Grondwet – namelijk de verklaring dat er grond bestaat een voorstel in overweging te nemen tot verandering in de Grondwet van de bepaling inzake de onschendbaarheid van het brief-, telefoon- en telegraafgeheim (Kamerstuk 2017, 33989, nr 334).

11 Daarnaast heeft de minister van BZK toegezegd om, indien er initiatieven vanuit de Tweede Kamer op het punt van horizontale werking van artikel 13 komen, deze waar mogelijk te ondersteunen (Kamerstukken 2016-2017, T02460, nr 33989). De horizontale werking van grond- en mensenrechten is de toepassing van grondrechten op de verhouding tussen burgers en betreffen privaatrechtelijke betrekkingen. De verticale werking is de toepassing van grondrechten op de verhouding tussen burgers en de overheid.

12 Zie: https://www.staatscommissieparlementairstelsel.nl/

digitalisering op de democratie, en naar mogelijke handelingsperspectieven van de overheid (Kamerstukken II 2017-2018, 34 775 VII, nr 52).

Tabel 3 Overzicht ontwikkelingen grondrechten Nederland, op hoofdlijnen (periode 1 januari 2017 - 30 juni 2018)

Wie/wat	Technologie	Issue	Actie
Staatscommissie parlementair stelsel	Sociale media, digitalisering	Bescherming democratie	Digitalisering als een van de zes thema's van de probleemverkenning
Regering	Digitalisering	Specifiek: vertrouwelijke communicatie	Grondwetswijziging artikel 13 in 2017
Ministerie van BZK	Algoritmen	Specifiek: impact van algoritmen op grondrechten	Onderzoek naar de impact van algoritmen op de effectiviteit van grondrechten
Ministerie van BZK	*Big data*, algoritmen en platformen	Specifiek: Bescherming democratie en daarmee verband houdende grondrechten	Adviesaanvraag Raad voor het Openbaar Bestuur digitalisering en democratie

Bron: Rathenau Instituut

2.2 Raad van Europa

In Europa heeft de Raad van Europa een actieve rol als 'hoeder' van de mensenrechten in Europa. Deze raad stelde in 1950 het Europese Verdrag voor de Rechten van de Mens op, en eind jaren tachtig speelde de raad een belangrijke rol op het gebied van ethiek en biotechnologie. In de periode 2017-2018 is de Raad van Europa op vele gebieden actief, bijvoorbeeld op het vlak van AI, geautomatiseerde gegevensverwerking, persuasieve technologie (via platformen en sociale media), ontwikkelingen in de biomedische industrie, robots en automatische wapens. We bespreken de relevante gebieden hieronder in meer detail.

Technologische convergentie
De Parlementaire Assemblee van de Raad van Europa (PACE) heeft onderzoek gedaan naar de betekenis van technologische convergentie (het steeds verder

integreren van mens en techniek) voor mensenrechten. In april 2017 kwam PACE met haar aanbevelingen aan de Raad van Ministers.[13] Ze stelde o.a. voor om:

1. de basisprincipes uit het Verdrag voor mensenrechten en biogeneeskunde,[14] zoals de bescherming van het privéleven, respect voor autonomie, en het recht op informatie, ook te laten gelden buiten de biomedische wereld, omdat digitalisering net als biotechnologie ingrijpt in de mens;
2. maatregelen te ontwikkelen voor het gebruik van zorgrobots en ondersteunende technologie, in de *Council of Europe Disability Strategy 2017-2023*.[15]
3. de noodzaak te erkennen dat elke machine, elke robot en elk kunstmatig intelligent artefact onder menselijke controle blijft;
4. nieuwe rechten aan te nemen gerelateerd aan het recht op respect voor het privéleven en familieleven:
    a. de mogelijkheid om te weigeren om geprofileerd, getrackt, gemanipuleerd of beïnvloed te worden; en
    b. het recht om, in het geval van zorg en begeleiding voor ouderen en mensen met een beperking, voor menselijk contact in plaats een robot te kunnen kiezen;
5. maatregelen in te voeren voor het gebruik van AI in de rechtszaal; en
6. met aanscherpingen te komen voor drones en andere kunstmatig intelligente systemen die gebruikt worden in een oorlog: er mogen geen geautomatiseerde procedures zijn voor het selecteren van individuen voor het doelgericht moorden gebaseerd op massale surveillancetechnieken.

De Raad van Ministers gaf in zijn reactie aan dat hij de nieuwe *Disability Strategy 2017-2023* heeft gelanceerd, met aandacht voor het gebruik van zorgrobots en *assisting technologies* en voor het voorkomen van discriminatie (Commissie van Ministers, 2017).[16] Verder zijn *big data*-richtlijnen aangenomen gericht op geautomatiseerde gegevensverwerking.[17] Overige aanbevelingen van PACE, bijvoorbeeld op het vlak van profilering en respect voor familieleven, heeft de Raad ofwel meegenomen in deze richtlijnen, ofwel neergelegd bij de Commissie voor Mensenrechten om deze aspecten mee te nemen bij de uitwerken van mensenrechten voor ouderen.[18]

---

13 De aanbevelingen werden opgesteld naar aanleiding van de motie *Technological convergence, artificial intelligence and human rights* (PACE, 2015). Op verzoek van PACE schreef het Rathenau Instituut en de rapporteur het rapport *Human rights in the robot age* (Van Est & Gerritsen, 2017), waarin het instituut o.a. pleit voor twee nieuwe mensenrechten: het recht om niet gemeten, geanalyseerd of beïnvloed te worden, en het recht op betekenisvol menselijk contact (Rathenau Instituut, 2017); zie ook: https://www.rathenau.nl/nl/digitale-samenleving/mensenrechten-het-robottijdperk

14 Dit verdrag is ook bekend als de 'Oviedo Conventie' (ETS No. 164). Zie: https://rm.coe.int/168007cf98

15 Zie ook: https://rm.coe.int/16806c400c

16 Zie: https://www.coe.int/en/web/disability/cyprus-conference-march-2017

17 Zie: https://rm.coe.int/16806ebe7a

18 CM(2014)2, Zie: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c68ce

Verder sloot de Raad aan bij de aanbevelingen van PACE voor de Commissie van Bio-ethiek (DH-BIO).[19] Er komt een actieplan om de impact van de ontwikkelingen in de biomedische industrie op mensenrechten in kaart te brengen, en op basis daarvan de doelen van DH-BIO te bepalen (DH-BIO 2017). Het plan moet mede gebaseerd worden op de uitkomst van de conferentie ter viering van het 20-jarig bestaan van het Verdrag voor mensenrechten en biogeneeskunde, in oktober 2017. Op de conferentie ging het vooral over de uitdagingen voor mensenrechten als gevolg van ontwikkelingen in het veld van genetica en *genomics*, en het gebruik van *big data* in de gezondheidszorg.[20]

Geautomatiseerde gegevensverwerking en AI

In 2017 stelde de Raad van Europa een expertgroep in die zich in 2018-2019 moet buigen over mensenrechten en geautomatiseerde gegevensverwerking. Dit *Committee of experts on Human Rights Dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT*)[21] volgt het *Committee of experts on Internet Intermediaries (MSI-NET)* op, die gericht was op verantwoordelijkheden van internetplatformen en geautomatiseerde gegevensverwerking. MSI-NET concludeerde in haar eindrapport '*Algorithms and human rights*' onder meer dat:

- publiek toezicht op geautomatiseerde gegevensverwerking wenselijk is; dit toezicht moet niet alleen worden overgelaten aan private partijen (Raad van Europa, 2018).
- publieke organisaties verantwoordelijk gehouden moeten worden voor de beslissingen die zij nemen op basis van algoritmische processen; en
- meer publiek debat nodig is over dit onderwerp.

De Commissie van Ministers van de Raad heeft naar aanleiding van dit rapport haar lidstaten opgeroepen tot verheldering van de verantwoordelijkheden van internetbedrijven en socialemediaplatforms (CM/Rec(2018)2).[22]

Digitalisering en de media

In 2017 richtte de Raad van Europa ook het *Committee of Experts on Quality Journalism in the Digital Age* op (MSI-JOQ) op.[23] Naast het voorbereiden van standaarden voor kwaliteitsjournalistiek in het digitale tijdperk, zal de commissie de

19 Zie: https://rm.coe.int/inf-2017-5-e-info-doc-dh-bio/168077c578
20 Zie ook: https://rm.coe.int/oviedo-conference-rapporteur-report-e/168078295c
21 Zie: https://www.coe.int/en/web/freedom-expression/msi-aut
22 https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2018-2-of-the-committee-of-ministers-to-member-states-on-the-roles-and-responsibilities-of-internet-intermediaries?inheritRedirect=false
23 Zie: https://www.coe.int/en/web/freedom-expression/msi-joq

komende twee jaar ook kijken naar mediawijsheid in een digitale omgeving. In de voorgaande periode 2016-2017 was het *Committee of experts on Media Pluralism and Transparency of Media Ownership (MSI-MED)* actief.[24] Dat richtte zich onder andere op transparantie van media-eigendom en het gebruik van internet in verkiezingen. De Commissie van de Ministers van de Raad van Europa benadrukte in reactie op de aanbevelingen van deze expertgroep het belang van de bestaande standaarden voor mediapluralisme en transparantie; ook vroeg ze de lidstaten dit kader regelmatig te beoordelen (CM/Rec(2018)1).[25]

Desinformatie en digitale veiligheid

Daarnaast waarschuwde PACE in de resolutie 2217 (2018) voor een nieuw 'gevaar van hybride oorlogen', waarbij gebruik wordt gemaakt van cyberattacks, massa-desinformatie, inmenging in verkiezingen, en ontwrichting van communicatienetwerken. Deze nieuwe bedreiging kan en moet worden bestreden binnen het nationale strafrecht, aldus PACE. Ook internationale normen met betrekking tot onder andere cybercrime en terrorisme zijn hiervoor van toepassing.[26]

Privacy

De Raad van Europa moderniseerde in 2018 het Dataprotectieverdrag (Personal Data Protection Convention 108).[27] Dat stamt uit 1981 en legde de basis voor de Europese privacybescherming. Het was en is het eerste bindende internationale instrument dat het individu beschermt tegen misbruik van het verzamelen en verwerken van persoonsgebonden data. De modernisatie plaatst privacy-uitdagingen in het licht van nieuwe informatie- en communicatietechnologieën en versterkt de mogelijkheden voor de Raad om de naleving van het verdrag te controleren.[28]

24 Zie: https://www.coe.int/en/web/freedom-expression/committee-of-experts-on-media-pluralism-and-transparency-of-media-ownership-msi-med-

25 Zie: https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2018-2-of-the-committee-of-ministers-to-member-states-on-the-roles-and-responsibilities-of-internet-intermediaries?inheritRedirect=false

26 Zie: http://assembly.coe.int/nw/xml/News/News-View-EN.asp?newsid=7059&lang=2&cat=8 en 'Legal challenges related to hybrid war and human rights obligations' http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24762&lang=en

27 Zie: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

28 Zie: https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet

Tabel 4 Overzicht ontwikkelingen grondrechten Europa op hoofdlijnen (periode 1 januari 2017 - 30 juni 2018)

Wie/wat	Technologie	Issue	Actie
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. Aanbevelingen ingediend door PACE
Parlementaire Assemblee van de Raad van Europa (PACE) motie	Hybride oorlog	Impact desinformatie en cybersecurity op de samenleving	Deze nieuwe bedreiging valt binnen bestaande wetten en juridische normen
Raad van Europa	Reactie op aanbevelingen van PACE	Breed: impact NBIC op mensenrechten	Aanbevelingen in de resolutie van PACE aangenomen
Raad van Europa (Steering Committee on Media and Information Society)	Digitalisering, platformen, AI	Vrijheid van meningsuiting, democratie	Commissie mensenrechten impact van algoritmen en AI (MSI-AUT), Commissie kwaliteitsjournalistiek digitale tijdperk (MSI-JOQ)
Raad van Europa	Digitalisering	Privacy	Modernisering van Dataprotectieverdrag (Convention 108)

Bron: Rathenau Instituut

2.3 Internationaal

De Mensenrechtenraad van de Verenigde Naties richt zich op de naleving van de mensenrechtenverdragen en kijkt naar de relatie tussen digitalisering en mensenrechten. In 2014 stelde de Mensenrechtenraad David Kaye aan als de Speciale Rapporteur op het gebied van het recht op vrijheid van meningsuiting, en in 2015 Joe Cannataci als eerste Speciale Rapporteur op het gebied van het recht op privacy.

Privacy
De VN-Mensenrechtenraad nam in de periode van 2012 tot 2017 drie resoluties aan met steeds kleine uitbreidingen.

1. De eerste resolutie, L13 *The promotion, protection and enjoyment of human rights on the Internet*, werd ingediend op 6 juli 2012.[29] Deze resolutie herbevestigd de Universele Verklaring van de Rechten van de Mens voor het digitale tijdperk door te benadrukken dat de rechten die mensen offline hebben ook online, in de digitale wereld, moeten worden beschermd.
2. Een tweede resolutie, L24, werd op 26 juni 2014 aangenomen, met als aanvulling de nadruk op het belang van het bestrijden van haat op het internet.
3. Naar aanleiding van de rapporten van de Speciale Rapporteurs[30] en de 2030 Agenda voor Duurzame Ontwikkeling heeft de VN-Mensenrechtenraad op 5 juli 2016 unaniem ingestemd met een derde resolutie, L20, met betrekking tot *The promotion, protection and enjoyment of human rights on the Internet*. De resolutie pleit ervoor dat online vrijheid als mensenrecht beschermd moet worden, en benadrukt het belang van toegang tot informatie op het internet.[31]

Big data en gezondheid

De Organisatie der Verenigde Naties voor Onderwijs, Wetenschap en Cultuur (UNESCO) gebruikt de werkterreinen onderwijs, wetenschap, cultuur en communicatie om de doelstellingen van de VN te realiseren, namelijk: ontwikkeling van universele waarden en verbetering van de leefomstandigheden van alle mensen ter wereld.[32] Binnen de UNESCO hebben het International Bioethics Committee (IBC) en de World Commission on the Ethics of Scientific Knowledge and Technology (COMEST) in 2017 rapporten gepubliceerd over *big data* en gezondheid, en robotica.

Met het rapport over *big data* en gezondheid signaleert het IBC (2017) dat governancesystemen voor *big data* de fundamentele rechten van mensen moeten beschermen, maar dat deze governancestructuur nog niet bestaat. Verantwoord gebruik maken van data en transparantie van algoritmen zijn daarbij cruciaal. Het IBC adviseert internationale organisaties:

- een wereldwijd juridisch raamwerk te creëren voor het gebruik van *big data* binnen de gezondheidzorg en –onderzoek;
- richtlijnen, ethische codes en ethiekcommissies te ontwikkelen op dit terrein.

29 Zie: http://geneva.usmission.gov/2012/07/05/internet-resolution

30 Op het gebied van het recht op privacy (A/HRC/34/60, 2017; A/HRC/31/64, 2016) en op het gebied van bescherming van het recht op vrijheid van meningsuiting op het internet (A/HRC/29/32, 2015; A/HRC/32/38, 2016)

31 Omdat toegang tot informatie het recht op onderwijs bevordert, en het de noodzaak voor digitale geletterdheid adresseert. Zie: http://www.osce.org/fom/250656

32 Zie: https://www.unesco.nl/unesco/unesco-wereldwijd

Robotica en ethiek

Met het rapport over robotica-ethiek signaleerde COMEST (2017) dat de groei van cognitieve robots[33] in de maatschappij leiden tot sociale en culturele veranderingen, en dat ze veiligheid, privacy en menselijke waardigheid onder druk kunnen zetten. COMEST wil meer bewustzijn creëren en een dialoog stimuleren over de ethische aspecten van het gebruik van autonome, cognitieve robots in de samenleving. Centrale kwesties zijn de autonomie van robots en de verantwoordelijkheid voor robots. COMEST adviseert:

- regulering van het gebruik van robots;
- ontwikkeling van ethische richtlijnen voor zowel producenten als gebruikers van robotica;
- integratie van ethiek in het ontwerpproces van robotica; en
- inzicht bij overheden en organisaties van de implicaties van robotica voor de arbeidsmarkt.

IoT en ethiek

COMEST bereidt ook een rapport voor over de ethische aspecten van het IoT. In voorbereiding hierop werd in samenwerking met de Universiteit Twente op 14 maart 2018 een workshop *Ethics of Internet of Things* georganiseerd, waarin werd gekeken naar de implicaties voor sociale interacties en machtsverhoudingen.[34]

Tabel 5 Overzicht ontwikkelingen grondrechten internationaal, op hoofdlijnen (periode 1 januari 2017 - 30 juni 2018)

Wie/wat	Technologie	Issue	Actie
VN-Mensenrechtenraad	Mensenrechten op het internet	Specifiek: mensenrechten op het internet	Internetresolutie L20
UNESCO, IBC	*Big data* & health	Breed: ethische kwesties	Rapport over *big data* & health
UNESCO, COMEST	Robotica	Breed: ethiek van robotisering	Rapport over robotica
COMEST	IoT	Breed: ethiek van IoT	Voorbereiding rapport

Bron: Rathenau Instituut

33 Cognitieve robots zijn robotica met menselijke vaardigheden zoals gewaarwording, taal, interactie, probleemoplossing, creativiteit, en leren. De belangrijkste eigenschap van cognitieve machines is dat hun handelingen onvoorspelbaar zijn. De vraag omtrent verantwoordelijkheid van handelingen van cognitieve robots is daarom van cruciaal belang.

34 Zie: https://www.utwente.nl/en/events/!/2018/3/188486/workshop-ethics-of-internet-of-things

2.4 Conclusie

In het domein van grond- en mensenrechten is de aandacht voor digitalisering en publieke waarden gegroeid ten opzichte van het rapport *Opwaarderen*, zowel op nationaal als op internationaal niveau. Waar voorheen in discussies over digitalisering en grondrechten met name aandacht was voor de opkomst van het internet en privacy en privacyrechten, is de discussie nu verbreed.

Dat geldt ook voor de discussie over het begrip ‘digitalisering’. Het gaat nu niet langer voornamelijk over internet en nieuwe communicatiemogelijkheden, maar ook over de inzet van digitale technologieën als *big data* en algoritmen, AI, platformen en persuasieve technologie en robotica.

Deze verbreding leidt ook tot een verbreding van de maatschappelijke en ethische kwesties die worden aangekaart. Zo staan nu ook zaken als vrijheid van meningsuiting, gelijke behandeling, autonomie en bescherming van democratie op de beleidsagenda.

Nederland
In Nederland is er al lange tijd aandacht voor digitalisering en privacyrechten. Het gaat dan met name om de opkomst van het internet en nieuwe communicatiemogelijkheden. Ook in 2017 en 2018 was hier aandacht voor. Er is – in eerste lezing – een grondwetswijziging aangenomen om de reikwijdte van artikel 13 uit te breiden naar alle communicatiemiddelen.

Daarnaast heeft de discussie zich verbreed naar nieuwe digitale technologieën, en daarmee ook naar andere publieke waarden. In 2017 heeft het ministerie van BZK laten onderzoeken hoe *big data*, algoritmen en AI niet alleen privacyrechten raken, maar ook vrijheidsrechten, gelijkheidsrechten en procedurele rechten. In het najaar van 2018 zal het kabinet zijn reactie op dit onderzoek naar de Tweede Kamer sturen.

Verder onderzoekt de Staatscommissie parlementair stelsel de invloed van *big data* en *microtargeting* in verkiezingscampagnes op fundamentele democratische waarden. Het ministerie van BZK heeft ook de Raad voor het Openbaar Bestuur gevraagd de effecten van digitalisering op de democratie te onderzoeken.

Internationaal
Ook internationaal is de aandacht voor privacy in relatie tot digitalisering (met name het internet) in de periode 2017-2018 bestendigd. Dat blijkt bijvoorbeeld uit de internetresoluties van de VN en de modernisering van Conventie 108 door de Raad van Europa. Daarnaast is er aandacht voor andere digitale technologieën, zoals

robotica en *big data*. Mensenrechteninstituties vragen aandacht voor kwesties als menselijke waardigheid, autonomie (agentschap) en controle over technologie (transparantie en verantwoordelijkheid). Ze roepen op tot bewustwording, en tot de ontwikkeling van nieuwe wettelijke kaders en ethische richtlijnen.

Nieuw op de agenda in 2017-2018 is de aandacht voor technologieën als AI en de effecten van geautomatiseerde besluiten. Ook is er aandacht voor platformen en sociale media, en de daarmee samenhangende maatschappelijke en ethische discussies over vrijheid van meningsuiting, media-eigendom, het democratisch stelsel, machtsverhoudingen, en digitale veiligheid en ontwrichting.

Er is, zowel nationaal als internationaal, weinig aandacht voor digitale technologieën, zoals biometrie (gezichtsherkenning en emotieherkenning) en *virtual* en *augmented reality*, en hun impact op mensenrechten.

3 Maatschappelijke actoren en debat

Met hun uitingen in het maatschappelijke en politieke debat geven burgers, maatschappelijke organisaties, belangenverenigingen en de media mede vorm aan hoe digitale technologie een plek krijgt in de maatschappij. Zij voeden de politiek-bestuurlijke en maatschappelijke discussie over digitalisering en kunnen daarmee een beleidsagenderende rol spelen. Ze zorgen er ook voor dat een breder publiek zich bewust is van diverse kwesties en dragen mogelijk ook bij aan (digitaal) empowerment van het individu. In dit hoofdstuk belichten we eerst enkele hoofdpunten van het debat in de media over digitalisering en publieke waarden, sinds het verschijnen van *Opwaarderen*. Dit is geen systematische nieuwsanalyse; we noemen slechts enkele opvallende gebeurtenissen op dit vlak. Vervolgens beschrijven we de kwesties die diverse maatschappelijke organisaties op de publieke en politieke agenda zetten.

In *Opwaarderen* zagen we dat er bij maatschappelijke organisaties veel aandacht was voor privacy en digitale veiligheid. Ook in de periode 2017-2018 was dat het geval. Burgerrechtenorganisaties ageerden bijvoorbeeld tegen de invoering van overheidsbeleid en -systemen, zoals de nieuwe Wet inlichtingen en veiligheidsdiensten (Wiv), de Wet Computercriminaliteit III en het risicoprofileringssysteem SyRi (Systematische Risico Index) dat als doel heeft om sociale verzekeringsfraude op te sporen.

Maar de discussie verbreedde zich ook. Maatschappelijke organisaties vroegen meer aandacht voor *big data*, algoritmen en AI, en de effecten van profilering. Ze kaartten kwesties aan als controle over technologie en rechtvaardigheid. In de media was er na de Brexit-campagne, de vermeende Russische inmenging in de presidentsverkiezingen in de Verenigde Staten en het Cambridge Analytica-schandaal veel aandacht voor de grote macht van technologiebedrijven. De rol van platformen bij het verspreiden van desinformatie werd aangekaart en er werden vraagtekens geplaatst bij de gevolgen van technologie op de geestelijke gezondheid van mensen. Toch zien we deze laatste thema's, desinformatie en de mogelijk verslavende werking van technologie, niet terug in de kwesties die Nederlandse maatschappelijke organisaties op de publieke en politieke agenda zetten.

3.1 Hoofdpunten uit het debat in de media

3.1.1 Nederland

Privacy
Een belangrijk aandachtspunt in Nederland was het wetsvoorstel voor de modernisering van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv). Op initiatief van een groep Amsterdamse studenten werd in 2017 een petitie gehouden om hierover een raadgevend referendum te houden. Daarvoor verzamelden de UvA-studenten eind 2017 voldoende handtekeningen. Veel belangenorganisaties onderstreepten dat ze vanuit privacyoverwegingen tegen (onderdelen van) de wet waren, en zetten zich in voor de tegencampagne.[35]

Begin 2018 klonk er ook kritiek op het leerlingvolgsysteem Magister. Volgens critici schendt dat systeem de privacy van leerlingen.[36] Na onderzoek constateerde de Autoriteit Persoonsgegevens (AP) dat de drie grote onderwijsorganisaties hun werkwijzen met een leerlingvolgsysteem zodanig hebben aangepast dat die voldoet aan de Wet bescherming persoonsgegevens.[37]

Ook de invoering van nieuwe EU-privacywetgeving, de Algemene verordening gegevensbescherming (AVG), leverde veel media-aandacht op. Na een aanloopperiode van twee jaar moesten bedrijven vanaf 25 mei 2018 aan de vereisten van de AVG voldoen. Er was in de media aandacht voor de nieuwe rechten voor burgers en plichten voor organisaties en bedrijven.[38] Daarnaast kwamen de problemen bij bedrijven en overheidsinstanties rond naleving van de AVG in het nieuws. Zo hadden veel kleine sportverenigingen met weinig vrijwilligers en middelgrote en kleine bedrijven hun datahuishouding vaak nog niet op orde.[39] Maar ook diverse ministeries voldeden bij invoering nog niet aan alle vereisten.[40] Bovendien meldden de media dat de AP met onderbezetting te maken had.[41]

35 Zie: https://sleepwet.nl/contact.html
36 Zie bijvoorbeeld https://www.trouw.nl/opinie/schoolsysteem-magister-is-bedreigend-opdringerig-en-ontneemt-leerlingen-hun-vrijheid~aa1a39ad/
37 Zie: https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/onderwijsorganisaties-passen-werkwijze-met-leerlingvolgsysteem-aan-na-onderzoek-ap
38 Zie: https://www.ad.nl/economie/dit-betekenen-de-nieuwe-privacyregels-voor-jou~ad49ee8b/
39 Zie: https://www.ad.nl/binnenland/duizenden-sportclubs-niet-klaar-voor-nieuwe-privacywet~af07644d/
40 Zie: https://www.rtlnieuws.nl/economie/ministeries-schenden-massaal-de-nieuwe-privacywet-avg
41 Zie: https://fd.nl/economie-politiek/1254871/onrust-bij-privacywaakhond-autoriteit-persoonsgegevens

Algoritmen en AI

Begin 2018 verscheen de robotrechter in het nieuws. Geschillen van klanten van onder andere zorgverzekeraars komen terecht bij het e-Court voor private rechtspraak. Er was kritiek op het gebrek aan transparantie: uitspraken werden niet gepubliceerd en het was niet bekend wie de 'rechters' zijn.[42] Naar aanleiding van de berichtgeving meldde het e-Court dat het versneld de vonnissen en de namen van arbiters op zijn website zou publiceren. De digitale rechter ligt op dit moment stil en kan geen geschillen meer beslechten.[43]

Media besteedden aandacht aan de mogelijk nadelige gevolgen van algoritmen en AI, zoals discriminatie of uitsluiting. NRC kwam met een serie over de rol van algoritmen op basis van eigen onderzoek. Ook het proefschrift van Marlies van Eck (2018) over 'geautomatiseerde ketenbesluiten & rechtsbescherming' en het rapport van de Stichting Kafkabrigade over ontsnappen uit 'De digitale kooi' (Widlak & Peeters, 2018) kregen veel aandacht.

Desinformatie

Met de aandacht voor de vermeende Russische invloed op de Amerikaanse presidentsverkiezing kwam er ook in Nederland aandacht voor desinformatie.[44] Er kwamen diverse initiatieven om de kwaliteit en betrouwbaarheid van berichtgeving te kunnen waarborgen en de transparantie te vergroten, zoals de samenwerking tussen Facebook, NU.nl en de Universiteit Leiden.[45] Sinds februari 2018 is de samenwerking tussen Facebook en deze universiteit echter opgeschort.[46] Het collectief DROG ontwikkelde een nepnieuwsspel om burgers weerbaarder te maken tegen desinformatie.[47]

Ook onderzochten media het gebruik van desinformatie door de media zelf.[48] Zo schreef NRC in juli 2018 dat zogenoemde nepaccounts vanuit Rusland actief berichten hebben verspreid om in Nederland verdeeldheid te zaaien.[49]

42 Zie: https://www.groene.nl/artikel/vonnis-te-koop
43 Zie: https://www.trouw.nl/home/digitale-geschillendienst-e-court-zit-zonder-geschillen~a843976c/
44 Desinformatie is onware, inaccurate of misleidende informatie die met opzet wordt gemaakt en verspreid om geld te verdienen of om een persoon, sociale groep, organisatie of land te schaden.
45 Daarbij verleent Facebook toegang aan NU.nl en de universiteit tot een speciaal Facebook-dashboard waarin artikelen te zien zijn die door gebruikers zijn aangemerkt als desinformatie
46 Zie: https://www.leidschdagblad.nl/leiden-en-regio/universiteit-leiden-schort-samenwerking-met-facebook-op-over-nepnieuws
47 Zie: https://www.slechtnieuws.nl/
48 Zie: https://www.nrc.nl/nieuws/2017/12/08/media-nederland-citeerden-trollen-als-bron-a1584306
49 https://www.nrc.nl/nieuws/2018/07/15/de-russische-trollen-zijn-anti-islam-en-voor-wilders-a1610155?_sp=7b4920fd-e289-4511-96a4-63a7868dae2b.1533730155032

Effecten op fysieke en mentale gezondheid
Tot slot was er aandacht voor de effecten op de mentale gezondheid van sociale media, naar aanleiding van onderzoek door het Centraal Bureau voor de Statistiek (CBS).[50] Van de jongvolwassenen – mensen tussen de 18 en 25 – beschouwt een steeds groter wordend percentage, 29%, zichzelf als verslaafd aan sociale media. Een deel van hen verklaarde tegenover het CBS dat ze zich minder goed kunnen concentreren, minder goed slapen en dat ze slechter presteren op school.[51]

Ook de fysieke gevolgen van sociale media, smartphones en tablets kwamen in het nieuws. Oogartsen waarschuwden voor de gevolgen van het gebruik van beeldschermen door kinderen. Het langdurig en veelvuldig gebruik van tablets en smartphones veroorzaakt volgens hen bijziendheid bij kinderen.[52] Ook kwam de 'tabletnek' in het nieuws. Volgens het Zorgkompas kampt een groot en groeiend aantal jongeren met nek- en rugklachten. Deze klachten worden veroorzaakt door de slechte houding tijdens smartphone- of tabletgebruik en het gebrek aan buitenspelen.[53]

3.1.2 Internationaal

In de internationale media was er veel kritiek op grote technologiebedrijven, van wetenschappers, oud-werknemers en investeerders tot de media zelf. Centraal stonden de ongelijke machtsverhoudingen en de verantwoordelijkheid van grote technologiebedrijven om iets te doen tegen de negatieve gevolgen van digitalisering.

Zo werd tijdens het World Economic Forum 2017 in Davos benadrukt dat de technologiemonopolies moeten worden aangepakt. Er werd gesteld dat zij, net als de sigarettenindustrie, verslavende en ongezonde producten maken.[54] Investeerders in Apple riepen het bedrijf op om werk te maken van software die het smartphonegebruik van kinderen inperkt.[55] Oud-werknemers van grote technologiebedrijven als Facebook, Apple en Google begonnen een *Truth about*

50 Zie: https://nos.nl/artikel/2211072-helft-12-16-jarigen-vindt-zichzelf-verslaafd-aan-sociale-media.html en https://www.nrc.nl/nieuws/2018/02/07/sociale-media-zijn-slecht-voor-gezondheid-kinderen-relaties-en-democratie-a1591341
51 Zie: https://www.cbs.nl/nl-nl/nieuws/2015/47/een-op-de-zes-jongeren-zegt-verslaafd-te-zijn-aan-sociale-media
52 Zie: https://www.nu.nl/gezondheid/5298404/meer-jongeren-mogelijk-bijziend-gebruik-smartphones-en-tablets.html
53 Zie: https://www.ad.nl/home/dag-muisarm-hier-is-de-tabletnek~acb3aecb/
54 Zie: http://www3.weforum.org/docs/FOP_Readiness_Report_2018.pdf en https://www.nesta.org.uk/blog/observations-davos-wef-2018 en https://www.nrc.nl/nieuws/2018/01/23/hoog-tijd-dat-overheden-techmonopolies-gaan-aanpakken-a1589467?utm_source=NRC&utm_medium=related&utm_campaign=related2
55 Zie: https://thinkdifferentlyaboutkids.com/

Tech-campagne en een *Centre for humane technology* om mensen bewust te maken van de 'donkere' kant van technologie, en de impact op de geestelijke gezondheid.[56] Ook moest Mark Zuckerberg, CEO van Facebook, zich na het Cambridge Analytica-dataschandaal[57] en de vermeende beïnvloeding van de Amerikaanse verkiezingen verantwoorden in het Amerikaanse Congres, en in het Europees Parlement.

In het voorjaar van 2018 lanceerden Apple en Google veelbeschreven nieuwe functies om smartphonegebruik in kaart te brengen, met als doel overmatig gebruik tegen te gaan.[58] Ook was er aandacht voor de opkomst van gezichtsherkenning en waren er zorgen over privacy en misbruik door de overheid. Zo riep Microsoft de Amerikaanse regering op om het gebruik van gezichtsherkenning (door overheden) te reguleren.[59]

Ten slotte publiceerden academici van 14 Amerikaanse instituten het rapport *The Malicious Use of Artificial Intelligence* (Brundage et al. 2018), om te waarschuwen tegen verkeerd gebruik van AI en om dat te beperken en te vermijden. Tesla-oprichter Elon Musk richtte in dit verband OpenAI op, een onderzoeksinstituut dat zich moet richten op een veilige ontwikkeling en toepassing van AI.[60]

3.2 Maatschappelijke organisaties

Hieronder geven we een overzicht van diverse relevante maatschappelijke actoren en hun initiatieven in 2017 en 2018. Privacy en digitale veiligheid staan in deze periode nog steeds prominent op de agenda. Bij digitale veiligheid verwijzen organisaties vaak naar de risico's van verbonden apparaten (IoT). Er kwamen ook nieuwe onderwerpen bij, zoals de risico's van profilering (zoals discriminatie en uitsluiting) en aandacht voor menselijke waardigheid, gekoppeld aan de inzet van algoritmen, geautomatiseerde besluitvorming en AI.

56 Zie: http://humanetech.com en https://www.volkskrant.nl/tech/oud-werknemers-facebook-en-google-beginnen-lobby-tegen-ontwrichtend-effect-van-sociale-netwerken~a4566913/ en https://www.nrc.nl/nieuws/2018/02/07/sociale-media-zijn-slecht-voor-gezondheid-kinderen-relaties-en-democratie-a1591341 en https://www.nrc.nl/nieuws/2018/01/08/aandeelhouders-apple-bezorgd-over-smartphoneverslaving-a1587522?utm_source=NRC&utm_medium=related&utm_campaign=related2

57 Zie: https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm?CMP=twt_gu

58 Bright.NL (2018) Hebben de nieuwe opties tegen telefoonverslaving zin? 6 juni 2018. Zie: https://www.bright.nl/trends/artikel/4224696/smartphone-verslaving-android-ios-12

59 Zie: https://www.theguardian.com/technology/2018/jul/14/microsoft-facial-recognition-technology-rules-potential-for-abuse

60 Zie: https://openai.com/about/

Consumentenbond

De Consumentenbond is een vereniging die zich inzet voor het belang en de rechten van consumenten, door middel van campagnes, acties, onderzoek en informatievoorziening. Online privacy en digitale veiligheid zijn belangrijke thema's voor de bond, die bijvoorbeeld in mei 2018 – vergeefs – in een rechtszaak eiste dat Samsung zijn telefoons gedurende de gehele gebruiksduur updatet.[61] De bond waarschuwde ook voor beveiligingslekken van babyfoons[62], en eerder voor de pop My Friend Cayla.[63]

Naar aanleiding van de invoering van de AVG publiceerde de bond in hoeverre Nederlandse websites de nieuwe privacyregels naleven – het bleek dat 2 op de 3 onderzochte websites de wet overtrad, aldus de bond.[64] Eerder voerde de Consumentenbond een steekproef uit onder 20 gezondheidswebsites. Advertenties werden getoond zonder toestemming van bezoekers. Mede op aandringen van de bond en de toezichthouder Autoriteit Consument- en Markt (ACM) is dit inmiddels veranderd.[65]

ECP Platform voor de informatiesamenleving

De stichting ECP heeft als missie het ondersteunen van een betrouwbare, kansrijke digitale samenleving in Nederland. Het is een platform met 130 leden, waaronder overheden, telecom- en ICT-bedrijven en maatschappelijke organisaties zoals de Consumentenbond. De vijf prioriteiten van ECP zijn gericht op 1) een betrouwbaar internet en de inzet van technologie in bedrijfs- en productieprocessen, 2) digitale veiligheid, vertrouwen in ICT en privacy, 3) digitale vaardigheden voor iedereen, 4) digitalisering in de zorgsector,[66] en 5) bewustzijn over het belang van digitalisering en de doorvertaling daarvan naar maatschappelijke domeinen en vraagstukken.

Op haar 20ste Jaarcongres presenteerde ECP twintig bouwstenen voor een kansrijke en betrouwbare digitale samenleving.[67] Nieuwe thema's voor het platform zijn AI en blockchaintechnologie. Daarover organiseerde het in 2018 diverse debatten, en publiceerde het een whitepaper (ECP, 2018). Ook organiseerde het diverse bijeenkomsten over blockchain en stond het aan de wieg van de 'Dutch

61 Zie: https://www.consumentenbond.nl/nieuws/2018/teleurstellende-uitspraak-in-rechtszaak-tegen-samsung
62 Zie: https://www.consumentenbond.nl/nieuws/2018/tienduizenden-foscam-camera%E2%80%99s-lek-direct-updaten-nodig
63 Zie: https://www.consumentenbond.nl/nieuws/2016/pratende-pop-cayla-slecht-beveiligd
64 Zie: https://www.consumentenbond.nl/nieuws/2018/2-van-de-3-websites-overtreden-nieuwe-privacywet
65 Zie: https://www.consumentenbond.nl/nieuws/2017/twee-op-de-drie-websites-overtreden-cookiewet
66 ECP heeft het initiatief genomen om een coalitie te vormen op het terrein van digitale competenties van werkenden in de zorg. De coalitie werkt vanuit het idee dat digitale vaardigheid bij alle groepen in het zorgsysteem goed moet zijn om serieus gebruik te kunnen maken van eHealth. Zie: https://digivaardigindezorg.nl/
67 Zie de 20 bouwstenen: https://ecp.nl/20bouwstenen/

Blockchain Coalition', met als doel om de uitrol van die technologie in Nederland te bevorderen.[68]

Culturele organisaties
Vanuit het culturele domein reflecteerden organisaties als Medialab SETUP, de Waag Society en V2_ op digitalisering, tijdens workshops, lezingen en exposities. Daarmee droegen ze bij aan het versterken van digitale vaardigheden bij het algemeen publiek.

Medialab SETUP besteedde veel aandacht aan algoritmen. Zo kwam het met een Algoritmisch Historisch Museum tijdens de Dutch Design Week 2017. Daarin werden algoritmes in een historische context geplaatst om bij bezoekers een kritische blik op hedendaagse algoritmes te creëren. In 2018 richtte het zijn blik op automatische beslissingen door algoritmen, in het programma 'Weapons of Math Retaliation'.[69] Daarin is naast de thema's *big data* en AI ook aandacht voor het gebruik van gezichtsherkenning (onder andere bij sollicitatiegesprekken).

De Waag Society richt zich op open en eerlijke technologie die niemand uitsluit. Hier waren in 2017 en 2018 *big data*, algoritmen en het IoT belangrijke aandachtspunten. Een deel van het onderzoeksprogramma voor 2018 richt zich op het inbouwen van ethiek in techniek (accountability), op het begrip digitale identiteit en op de zeggenschap van burgers in smart cities.

Ook bij V2_, een instituut voor kunst en mediatechnologie, was er in 2017 en 2018 aandacht voor *big data*, algoritmen en profilering. Een van de initiatieven in 2017 was 'The Black Box Concerns', over de ondoorzichtigheid van slimme algoritmen. Ook in 2018 zal V2_ aandacht hebben voor dit thema (V2 2018).

Burgerrechtenorganisaties
Nederland kent diverse burgerrechtenorganisaties, zoals Bits of Freedom, Privacy First en Vrijbit, die zich onder meer inzetten voor online privacy en toegang tot informatie. In de periode 2017-2018 voerden zij met name campagne tegen de invoering van de Wet inlichtingen- en veiligheidsdiensten (Wiv) en de Wet Computercriminaliteit III. Ook werkten diverse organisaties samen om een procedure aan te spannen tegen de Nederlandse staat over het zogenoemde System Risico Indicatie Systeem, SyRI. Dit systeem is bedoeld om fraude met sociale verzekeringen op te sporen, en kan diverse gegevensbestanden van diverse instanties, (zoals gemeenten, UWV, SVB, Inspectie SZW en de Belastingdienst), koppelen voor dit doel. Het systeem analyseert de gegevens en komt met risicomeldingen over verdachte personen of bedrijven. De betrokken

68 Zie: https://www.dutchdigitaldelta.nl/blockchain
69 Zie: https://www.setup.nl/magazine/2018/01/civil-weapons-math-retaliation

instanties onderzoeken de melding van het systeem verder (Kamerstukken 2016-2017, 26643 en 32761, nr. 426).

De kwesties die de organisaties aankaartten gingen niet alleen over het verzamelen van persoonsgegevens, maar vooral over nieuwe technieken om data te analyseren en groepen mensen te profileren. Daarmee vroegen ze aandacht voor kwesties als behoud van autonomie, controle over technologie, rechtvaardigheid, menselijke waardigheid en machtsverhoudingen.

Stichting **Bits of Freedom** is een digitale burgerrechtenbeweging, die zich sinds 1999 richt op het beschermen van (communicatie)vrijheid en privacy op het internet. Dit doet ze via campagnes, lobby's, rechtszaken en de ontwikkeling van *tools*. Een van de bekendste campagnes is de jaarlijkse uitreiking van de Big Brother Awards. In 2017 ontving het kabinet er een, voor de Wet op de inlichten- en veiligheidsdiensten (Wiv). De stichting voerde er in 2017 actief campagne tegen, net als tegen de Wet Computercriminaliteit III.

Verder zette zij zich in voor het gebruik van versleuteling en netneutraliteit.[70] In mei 2017 riep Bits of Freedom de Autoriteit Consument en Markt (ACM) op om met scherpe acties de naleving van netneutraliteitsregels af te dwingen, en zo de vrijheid van de internetter te blijven beschermen. Daarnaast organiseerde de stichting regelmatig Privacy Cafés, waar mensen zich kunnen laten voorlichten over veilig en vrij internetten. Met *My Data Done Right* ontwikkelde Bits of Freedom een *open source tool* waarmee burgers meer transparantie kunnen afdwingen bij partijen die hun data gebruiken.

De stichting **Privacy First** is in 2008 opgericht als onafhankelijke stichting ter behoud en bevordering van het recht op privacy. Ze probeert privacyschendingen tegen te gaan via politieke lobby, publiekscampagnes of juridische acties en rechtszaken. Ook organiseert ze jaarlijks de 'Privacy Awards' voor Nederlandse organisaties die op een positieve manier met privacy omgaan. Belangrijke onderwerpen zijn privacy en geheime diensten (campagne tegen de Wiv), *big data* en profilering, privacy, autonomie en mobiliteit in het openbare domein. In 2017 en 2018 kwam daar het thema kinderen en privacy (met het oog op toenemend gebruik digitale leeromgevingen in het onderwijs) bij, en de financiële sector in relatie tot privacy. Voor dat laatste ontwikkelt Privacy First samen met de Volksbank in 2018 een keurmerk voor de bancaire en fintechsector, met het oog op de nieuwe Europese richtlijn voor betaaldiensten (de *Payment Service Directive 2*).[71]

70 Netneutraliteit is het beginsel dat internetproviders alle gegevens gelijk behandelen, en niet discrimineren naar gebruiker, inhoud, website, type toepassing en dergelijke. Zie: https://www.bof.nl/dossiers/netneutraliteit/

71 Interview met Privacy First, 7 mei 2018.

Juridische procedures vormen een belangrijk middel voor de stichting, in 2017-2018 o.a. tegen SyRi, automatische nummerplaatherkenning (ANPR) en kentekenparkeren. Het ANPR-wetsvoorstel werd op 21 november 2017 door de Eerste Kamer aangenomen. Het regelt dat politie kentekengegevens (zoals het kenteken, locatie, tijdstip, en foto van het voertuig) mag vastleggen en bewaren, voor vier weken.[72] In juni 2017 stapte Privacy First naar de rechter over het kentekenparkeren, omdat hiervoor volgens de stichting een wettelijke basis ontbreekt en burgers niet meer anoniem kunnen parkeren. In oktober 2017 wees de rechter de zaak af. Privacy First is in hoger beroep gegaan.[73]

Burgerrechtenvereniging **Vrijbit** zet zich in voor het recht op privacy, vrije communicatie en toegang tot informatie. Net als andere burgerrechtenorganisaties verzette ook Vrijbit zich in 2017 en 2018 tegen de Wiv. Om aan te geven dat die het recht op bescherming van het privéleven en lichamelijke integriteit van Nederlanders aantast, stuurde ze onder andere een brief naar de Hoge Commissaris van de Mensenrechten van de VN.[74]

Daarnaast bereidde ze juridische acties voor. Zo zette Vrijbit zich in om de Paspoortwet zodanig te laten aanpassen dat er geen biometrische persoonsgegevens meer worden toegepast voor de uitgifte van paspoorten en ID-kaart documenten. Na bij de Raad van State gedeeltelijk in het gelijk te zijn gesteld, zet de organisatie de strijd momenteel voort bij het Europees Hof voor de Rechten van de Mens.[75] Ook heeft Vrijbit met succes meerdere juridische rechtszaken aangespannen tegen de Autoriteit Persoonsgegevens (AP). Volgens de vereniging treedt die onvoldoende handhavend op tegen het onrechtmatig gebruik van medische persoonsgegevens.[76]

72 Zie: https://www.privacyfirst.nl/rechtszaken-1/item/1097-privacy-first-begint-rechtszaak-tegen-wetsvoorstel-anpr.html

73 Zie: https://www.privacyfirst.nl/rechtszaken-1/kentekenparkeren/item/1077-nieuwe-rechtszaak-over-anoniem-parkeren-met-contant-geld.html

74 Zie: https://www.vrijbit.nl/dossiers/dossier-wet-en-regelgeving/item/1065-vrijbit-brief-aan-de-hoge-commissaris-van-de-mensenrechten-van-de-vn.html

75 Zie: https://www.vrijbit.nl/dossiers/dossier-paspoortwet/item/1085-vingerafdrukken-weg-uit-paspoort-wachten-op-uitspraak-ehrm-of-wil-de-nieuwe-paspoort-piet-in-de-tweede-kamer-opstaan.html

76 Zie de rechtszaak over het gebruik van een gedragscode die door de rechter als onrechtmatig werd verklaard, de rechtszaak over het niet optreden van de AP tegen het Diagnose Informatie Systeem (DIS) door de Nederlandse Zorgautoriteit en procedures om de AP handhavend te laten optreden tegen de beheerder van het EPD-LSP-systeem: https://www.vrijbit.nl/dossiers/dossier-gezondheidszorg/item/1058-persbericht-vrijdagmiddag-10-maart-dienen-in-utrecht-2-rechtszaken-over-onrechtmatig-verzamelen-en-verwerken-van-ieders-medische-gegevens-door-de-zorgverzekeraars-en-nederlandse-zorg-autorit en https://www.privacybarometer.nl/nieuws/3909/Rechter_geeft_Autoriteit_Persoonsgegevens_er_van_langs

Een **groep maatschappelijke organisaties**, bestaande uit Privacy First, het Nederlands Juristencomité voor de Mensenrechten,[77] Platform Bescherming Burgerrechten[78] en de Landelijke Cliëntenraad, spande op 27 maart 2018 een procedure aan tegen de Nederlandse staat over het fraudeopsporingssysteem SyRI.[79] Volgens de coalitie vormt het risicoprofileringssysteem een risico voor de democratische rechtstaat. Volgens de coalitie is het voor de burger onduidelijk welke gegevens het systeem gebruikt, welke analyses daarmee worden uitgevoerd en wat hem of haar al dan niet tot risico maakt. Diverse verzoeken om informatie, verwijzend naar de Wet openbaarheid bestuur, leverden de organisaties weinig informatie op. Volgens het ministerie van Sociale Zaken en Werkgelegenheid zouden calculerende burgers, wanneer de gebruikte gegevens en risicomodellen vrijgegeven zouden worden, weten waarop ze moeten letten wanneer zij fraude plegen (SZW, 2018). Volgens de eisers is dit in strijd met onder meer de informatieplicht en het recht op een eerlijk proces.

Amnesty International Nederland strijdt voor mensenrechten. Sinds 2017 kijkt de organisatie ook naar het gebruik van algoritmes en AI, bijvoorbeeld door de politie, en de risico's die deze met zich meebrengen (zie ook paragraaf 3.4). Amnesty vindt dat er discussie nodig is over hoe de overheid omgaat met AI. Ze maakt zich bijvoorbeeld zorgen over de *bias* in algoritmen, en over het gebrek aan transparantie over wat systemen doen.[80]

77 Het Nederlands Juristen Comité voor de Mensenrechten (NJCM) zet zich in voor de bescherming van mensenrechten in Nederland en het Nederlandse buitenlandbeleid. Het Comité had aandacht voor de Wiv, de Wet Computercriminaliteit III, en de wetswijziging van artikel 13 van de Grondwet

78 Het Platform Bescherming Burgerrechten is een netwerk van organisaties, groepen en personen die streven naar een betere waarborging en versterking van de burgerrechten in Nederland. Thema's zijn onder andere biometrie in het paspoort, privacy in de gezondheidszorg en profilering

79 SyRI is een systeem van de overheid dat persoonsgegevens van burgers aan elkaar koppelt met de bedoeling om fraude, misbruik en overtredingen op te sporen. Het is een uitwerking van de wet SUWI (Structuur Uitvoeringsorganisaties Werk en Inkomen) die aangenomen werd in 2013.

80 Zie: https://www.rathenau.nl/nl/digitale-samenleving/amnesty-international-algoritmes-moeten-zich-aan-de-mensenrechten-houden

Tabel 6 Overzicht ontwikkelingen maatschappelijke organisaties, op hoofdlijnen (periode 1 januari 2017 - 30 juni 2018)

Wie/wat	Technologie	Issue	Actie
Consumenten-bond	Internet, apps, consumenten-elektronica, IoT	Privacy, digitale veiligheid	Campagne privacybewustzijn. Rechtszaak beveiligingsupdates, medische dataopslag en privacy
ECP	Digitalisering Blockchain, AI	Digitale veiligheid, privacy, inclusiviteit	O.a. Programma's voor digitale skills en veiligheid, blockchain, werkgroep gedragscode AI
Culturele organisaties			
SETUP	Algoritmen, AI, gezichtsherken-ning	Controle op technologie, rechtvaardigheid	Algoritmisch Historisch Museum, Weapons of Math Retaliation
De Waag Society	*Big data*, algoritmen IoT	Privacy, autononomie, controle over technologie, menselijke waardigheid, machtsverhoudingen	O.a. Digitale Identiteitslab, Waag Makerbox
V2_	AI, digitale platforms, *big data*, algoritmen en profilering	Menselijke waardigheid, privacy, autonomie	O.a. The Black Box Concerns, Test_Lab, 3x3
Burgerrechtenorganisaties			
Bits of Freedom	Internet, digitale communicatie	Privacy, digitale veiligheid, vrijheid van communicatie	Big Brother Awards, privacycoalitie, internetvrijheid toolbox, Wiv 2017, Computercriminaliteit III, netneutraliteit, My Data Done Right
Privacy First	Digitale communicatie, digitale overheid	Privacy, *big data*, profilering	Juridische acties opslag telecomgegevens, SyRI risicoprofilering, ANPR Keurmerk financiële diensten
Burgerrech-tenvereniging Vrijbit	Internet, digitale overheid	Privacy, vrije communicatie en toegang tot informatie, mensenrechten	Wiv 2017, Paspoortwet, onrechtmatig verzamelen van medische gegevens
Amnesty International Nederland	Algoritmen, AI	Controle op technologie, rechtvaardigheid, mensenrechten	Risico's van het gebruik van algoritmen voor mensenrechten, o.a. bij de politie

Bron: Rathenau Instituut

3.3 Koepelorganisaties bedrijfsleven en werknemers

Hieronder bespreken we diverse beroeps- en koepelorganisaties die het bedrijfsleven, programmeurs en professionals vertegenwoordigen. Deze organisaties besteedden in 2017-2018 aandacht aan privacy en digitale veiligheid, onder andere met het oog op aankomende, of net ingevoerde, Europese wetgeving, zoals de Algemene verordening gegevensbescherming (AVG), de ePrivacy-verordening (dit voorstel bevat specifieke privacyregelgeving voor de elektronische communicatiesector, die o.a. ook moeten gaan gelden voor nieuwe platformen zoals Whatsapp, Facebook Messenger en Skype) en de Cyber Security Act (zie ook hoofdstuk 5). Ook was er aandacht voor AI en de toekomst van werk. Voorzichtig kwam er ook discussie over ethiek en grondrechten op gang, bijvoorbeeld bij Nederland ICT en bij de beroepsvereniging voor informatieprofessionals KNVI.

Werkgeversorganisatie **VNO-NCW** behartigt de belangen van het Nederlandse bedrijfsleven. Op het gebied van digitalisering besteedde de organisatie in 2017 en 2018 aandacht aan privacy en digitale veiligheid.[81] Zo ontwikkelde ze samen met **MKB-Nederland** de Privacy Quick Scan.[82] Beide organisaties waren in deze periode bezig met het voorlichten en voorbereiden van het bedrijfsleven op de nieuwe privacywetgeving (AVG). Eerder al, eind 2016, werd een campagne begonnen tegen cybercrime, met onder meer het project Veilig Zakelijk Internetten. Daarmee kunnen ondernemers de veiligheid van hun digitale omgeving laten testen.[83]

Nederland ICT is de belangenvereniging en vertegenwoordiger van de Nederlandse ICT-sector. Ze besteedt aandacht aan onder andere privacy, veiligheid (vertrouwen) en digitale vaardigheden, onder meer, ter voorbereiding op de AVG, met de ‘Helpdesk AVG’ en de ‘AVG Toolkit’. In de periode 2017-2018 kwam ethiek als nieuw thema op de agenda.

Een van speerpunten van de **Vakcentrale voor Professionals (VCP)** is AI, omdat die technologie grote invloed heeft op de ontwikkelingen op de arbeidsmarkt. De VCP vindt dat professionals zich blijvend moeten kunnen ontwikkelen en wil aandacht voor de gevolgen van AI voor de verdeling van werk en inkomen.[84]

81 https://www.vno-ncw.nl/standpunten/privacy
82 https://www.vno-ncw.nl/standpunten/privacy
83 Zie: https://www.vno-ncw.nl/projects/veilig-zakelijk-internetten
84 Eind 2016 had het VCP-symposium AI als thema.

De **FME**, de ondernemersorganisatie voor de technologische industrie, heeft Berenschot en TIAS in 2017 onderzoek laten doen naar de invloed van technologische ontwikkelingen op werk in de technologische industrie (zoals robotisering en IoT). Aan dit onderzoek werkten ruim 6.900 medewerkers mee. In het daaruit volgende rapport *Onderzoek Smart Working* (Hos et al. 2018) worden de veranderende banen en taken besproken.[85] De meerderheid van ondervraagde medewerkers denkt dat digitalisering niet tot het verdwijnen van banen zal leiden, maar juist tot nieuwe en andere werkgelegenheid. Het rapport geeft aan dat nieuwe technologie vraagt om andere vaardigheden en kennis, waardoor een leven-lang-leren belangrijker wordt. De meeste ondervraagde medewerkers voelen zich verantwoordelijk om bij te blijven, en willen betrokken worden bij de ontwikkelingen.

De Nederlandse beroepsvereniging voor informatie- en IT-professionals **KNVI** is een onafhankelijk platform voor het ontwikkelen en uitwisselen van vakkennis en het verbreden van het netwerk van de leden. Ze werkt met jaarthema's; voor 2018 is dat *Smart Humanity*, om te wijzen op de blijvende centrale positie van de mens. Het staat voor mensen die digitale ontwikkelingen toepassen, en voor een samenleving die hiermee ethisch verantwoord omgaat.

De KNVI speelt ook een rol bij het agenderen van kennis en scholing en is vakinhoudelijk betrokken bij de uitvoering.[86] Ze ziet voor IT-professionals een cruciale rol om digitalisering in goede banen te leiden en om kenbaar te maken wanneer grondrechten in het geding komen.[87] Daarom wil ze dit jaar een dialoog hierover beginnen met het bedrijfsleven, de wetenschap en de politiek.

Het **Wetenschappelijk Bureau voor de Vakbeweging – De Burcht** heeft in 2018 het rapport *Samen werken met robots* uitgebracht. De studie behandelt de gevolgen van automatisering, digitalisering en robotica voor banen, werknemers en de veranderende rol van vakbonden (Freese & Dekker, 2018).

De **Federatie Nederlandse Vakbeweging (FNV)** heeft in 2017 een proefproces aangevraagd tegen het bedrijf Uber, omdat het oneerlijke concurrentie met andere taxichauffeurs in de hand zou werken. Naar aanleiding daarvan bepaalde een rechter dat Uberchauffeurs geen zelfstandige ondernemers zijn.[88] Eerder verenigden taxichauffeurs in Spanje zich tegen het bedrijf.[89] Dat leidde tot een

85 Zie: https://www.fme.nl/nl/nieuws/medewerkers-industrie-laat-robots-komen
86 Zie: https://www.knvi.nl/persbericht-smart-humanity/
87 Zie: https://www.rathenau.nl/nl/digitale-samenleving/knvi-geef-iters-de-ruimte-om-schending-grondrechten-te-benoemen
88 Zie: https://www.parool.nl/amsterdam/fnv-wil-zaak-tegen-uber-starten-maar-chauffeurs-durven-niet~a4542336/
89 Zie: https://www.politico.eu/article/tito-alvarez-uber-battle-ecj-decision/ en https://www.politico.eu/article/uber-ecj-ruling/

rechtszaak waarbij uiteindelijk, op 20 december 2017, het Hof van Justitie van de Europese Unie bepaalde dat de dienst die Uber via een app aanbiedt een vervoersdienst is in de zin van het EU-recht, en geen (digitale) dienst (Hof van Justitie van de Europese Unie, 2017).[90] Dit betekent dat de EU-lidstaten nationaal mogen bepalen onder welke voorwaarden deze dienst mag worden verleend.[91]

Tabel 7 Overzicht ontwikkelingen koepelorganisaties bedrijfsleven en werknemers, op hoofdlijnen (periode 1 januari 2017 - 30 juni 2018)

Wie/wat	Technologie	Issue	Actie
OESO-richtlijnen maatschappelijk verantwoord ondernemen	Specifiek case by case	Specifiek case by case	Bedrijven hebben een zorgplicht om mensenrechten te respecteren
VNO-NCW / MKB-Nederland	Digitalisering	Privacy, digitale veiligheid	Project Veilig Zakelijk Internetten
Nederland ICT	Digitalisering	Privacy, digitale veiligheid, ethiek	Helpdesk Avg en de Avg Toolkit
VCP	AI	Arbeidsmarkt, menselijke waardigheid	Invloed van AI op verdeling van werk en inkomen
KNVI	Digitalisering	Digitale vaardigheden, ethiek en grondrechten	Focus op Smart Humanity
De Burcht	Robotica	Arbeidsmarkt	Gevolgen digitalisering, automatisering en robotica voor banen, werknemers en de rol van vakbonden
FME	Digitalisering	Arbeidsmarkt	Digitalisering leidt tot nieuwe en andere werkgelegenheid
FNV	Platform- en deeleconomie	Machtsverhoudingen	Proefproces tegen Uber
Spaanse taxi-chauffeurs	Platform- en deeleconomie, locatie- en telecomgegevens	Privéleven, democratische waarden	Uitspraak dat Uber een taxibedrijf en geen techbedrijf is

Bron: Rathenau Instituut

90 Zie: Artikel 58 TFEU: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT

91 Zie: vragen van het lid Gijs van Dijk (PvdA) aan de Ministers over de uitspraak van het Europese Hof van Justitie dat Uber een taxibedrijf is (ingezonden 8 januari 2018): https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2018D04785&did=2018D04785

3.4 Internationale ontwikkelingen

Internationaal voeren maatschappelijke organisaties een levendige discussie over de ethiek van digitalisering, met name op het gebied van mensenrechten en AI. **Privacy International**, een non-profit- en non-gouvernementele organisatie, heeft samen met mensenrechtenorganisatie **Article 19** in april 2018 een rapport uitgebracht dat de risico's benadrukt van AI voor het recht op vrijheid van meningsuiting en het recht op privacy (Privacy International & Article 19, 2018). Volgens het rapport moet overheidsbeleid mensenrechten beschermen; zorgen voor verantwoordelijk en transparantie omtrent AI, en overheden stimuleren om de adequaatheid van juridische en beleidsraamwerken te herzien.

Het **European Digital Rights Initiative (EDRi)**, een vereniging van civiele en mensenrechtenorganisaties die rechten en vrijheden in het digitale tijdperk wil beschermen, is actief op het gebied van privacy, gebruik van biometrie in identificatiemiddelen, desinformatie, digitale veiligheid en controle over technologie.

Amnesty International heeft in 2017 een *Artificial Intelligence and Human Rights Initiative* opgericht om zowel mensenrechtenbeginselen te formuleren voor AI als de discussie over de ethiek van AI aan te zwengelen.[92] Ook is Amnesty een campagne begonnen tegen het ontwikkelen van killer robots.[93] Verder is ze zich gaan richten op de vraag hoe AI wereldwijde uitdagingen op het gebied van mensenrechten kan helpen oplossen.

Belangrijke onderwerpen van het Bureau van consumentenverenigingen **BEUC**, zijn digitale consumentenrechten, onder andere op het vlak privacy en security online en het IoT, netneutraliteit en geoblocking.[94] Een nieuw thema voor het BEUC is AI. In juni 2018 publiceerde de organisatie haar standpunt over geautomatiseerde gegevensverwerking en AI (BEUC 2018a). Ze pleit onder andere voor een *AI Consumer Action Plan*, waarin de Europese Commissie bekijkt of en waar aanpassingen aan het bestaande juridische kader nodig zijn om consumenten beter te kunnen beschermen.[95]

Het BEUC leverde ook input voor de voorstellen van de Europese Commissie om het consumentenrecht in de Europa te moderniseren (BEUC 2018b). Het vindt dat er nieuwe consumentenrechten nodig zijn met het oog op IoT, AI en algoritmen. Zo

92 Zie: https://www.amnesty.org/en/latest/news/2017/06/artificial-intelligence-for-good/
93 Zie: https://www.stopkillerrobots.org
94 Bij geoblocking krijgen online klanten geen toegang tot de diensten of producten van een website in een andere EU-lidstaat.
95 De organisatie vindt verder dat er meer er meer mogelijkheden moeten komen voor consumenten om inzicht te krijgen in geautomatiseerde besluitvorming en er bezwaar tegen te maken, en dat er meer duidelijkheid moet komen over aansprakelijkheid van bedrijven die geautomatiseerde besluitvorming inzetten.

moeten er collectieve procedures komen voor het schadeloos stellen van consumenten. Ook stelde de BEUC aanpassingen voor op het gebied van informatievoorziening (over hoe algoritmen functioneren, en hoe informatie en prijzen worden gerangschikt en gepresenteerd aan consumenten) en op het vlak van aansprakelijkheid (BEUC 2018a).

Verder publiceerde het BEUC zijn opmerkingen op de Cybersecurity Act. Het vroeg om meer aandacht voor IoT en de veiligheid van verbonden producten en diensten. Volgens het BEUC moeten consumenten verplicht veiligheid *by design* krijgen (BEUC 2018c). Minimale bindende eisen zouden volgens het BEUC moeten zijn: verplichte software updates, verplicht gebruik van sterke authenticatiemechanismen en van encryptie.

Tot slot publiceerde het BEUC, samen met onder andere de internationale organisatie voor consumentengroepen **Consumers International**, principes om privacy, veiligheid en beveiliging de belangrijkste kenmerken van IoT te maken.[96].

De internationale organisatie voor technische professionals **IEEE** doet vanaf 2017 onderzoek naar de attitudes van ouders ten op zichte van de interactie tussen kinderen en intelligente systemen.[97] Met het initiatief *Ethics in Action* wil de organisatie ontwikkelaars van autonome systemen ondersteunen bij het maken van ethisch verantwoorde keuzes en hiervoor ethische richtlijnen ontwikkelen.[98] Eind december 2017 verscheen de tweede versie van deze ethische richtlijnen voor autonome en intelligente systemen. In 2018 wordt feedback op de richtlijnen verzameld.

96 Zie: https://www.consumersinternational.org/media/154809/iot-principles_v2.pdf
97 Zie: https://www.ieee.org/about/news/2017/ieee-unveils-generation-ai.html
98 Zie: https://ethicsinaction.ieee.org

Tabel 8 Overzicht ontwikkelingen internationale organisaties, op hoofdlijnen (periode 1 januari 2017 - 30 juni 2018)

Wie/wat	Technologie	Issue	Actie
EDRi (EU)	Internet, AI	Mensenrechten online, vrijheid van meningsuiting	Privacy, biometrie in identificatie, desinformatie, digitale veiligheid
Privacy International	Internet, AI	Privacy, vrijheid van meningsuiting	Beleid moet mensenrechten beschermen en zorgen voor transparantie en verantwoordelijkheid rondom AI
Amnesty International	AI, robotisering	Mensenrechten	Mensenrechtenbeginselen formuleren voor AI Campagne tegen killer robots
BEUC en Consumers International	Digitalisering, IoT, AI	Privacy, cybersecrity, consumentenrecht, controle over technologie	AI Consumenten Actie Plan Privacy en veiligheid Principes IoT
IEEE (int.)	AI, algoritmen, robotica	Ethiek autonome systemen-	Initiatief om ontwerpers van autonome systemen te helpen ethische keuzes te maken Kinderen en AI

Bron: Rathenau Instituut

3.5 Conclusie

Veel aandacht voor privacy en digitale veiligheid

Nederlandse maatschappelijke organisaties hadden in de periode 2017-2018 veel aandacht voor privacykwesties en digitale veiligheid. Burgerrechtenorganisaties richtten zich op campagnes en rechtszaken tegen het Nederlandse overheidsbeleid, zoals de invoering van de nieuwe Wet inlichtingen en veiligheidsdiensten (Wiv), de Wet Computercriminaliteit III en digitale systemen van de overheid, zoals SyRi en ANPR (kentekenregistratie). De organisaties vroegen niet alleen aandacht voor dataverzameling, maar ook voor nieuwe technieken om data te analyseren en mensen te profileren, en de mogelijke risico's daarvan. Profilering raakt zo aan kwesties als autonomie, controle over technologie,

rechtvaardigheid en menselijke waardigheid. De Consumentenbond agendeerde met name privacy online, en de veiligheid van verbonden apparaten bij het IoT.

AI en mensenrechten als nieuw thema

Met de opkomst van *big data*, algoritmen en AI groeit ook de aandacht voor de betekenis van die technologieën voor mensenrechten. Diverse organisaties maken van AI en mensenrechten een nieuw thema binnen hun organisatie, zoals Amnesty International, medialab SETUP of de Europese consumentenorganisatie BEUC deden. In vergelijking met het rapport *Opwaarderen* staan thema's als controle over technologie, menselijke waardigheid en rechtvaardigheid dus veel nadrukkelijker op de agenda van maatschappelijke organisaties. Ook bij koepelorganisaties voor het bedrijfsleven is de aandacht voor dit thema voorzichtig gegroeid.

Niet op de agenda

Waar de media relatief veel aandacht besteden aan de macht van platformen, sociale media en desinformatie en bescherming van democratische stelsels, en zaken als persuasieve technologie in sociale media en apps en effecten op de geestelijke gezondheid van mensen, zien we deze thema's niet terugkomen op de agenda's van Nederlandse maatschappelijke organisaties. Ook zien we nauwelijks discussie op gang komen over *virtual* en *augmented reality*. Verder is er, met uitzondering van de aandacht voor biometrische toepassingen in paspoorten, betrekkelijk weinig aandacht voor biometrische ontwikkelingen, terwijl met name de ontwikkelingen en toepassingen op het vlak van gezichtsherkenning zich in snel tempo ontwikkelen. Tot slot lijkt ook robotica op nationaal niveau minder prominent op de agenda te staan.

4 Politiek en bestuur: agendavorming

Binnen het politiek-bestuurlijk domein bespreken we de publicaties van diverse nationale adviesraden, planbureaus en instituten die maatschappelijke en ethische kwesties op het gebied van digitalisering signaleerden en deze op de beleidsagenda zetten. Vervolgens bespreken we enkele internationale adviesorganisaties die als taak hebben ethische en maatschappelijke kwesties rondom digitalisering in kaart te brengen.

Omwille van de leesbaarheid behandelen we in dit hoofdstuk ook de kabinetsreacties op diverse adviezen. In hoofdstuk 5 komen we daar kort op terug.

Sinds *Opwaarderen* vragen meer adviesraden aandacht voor de betekenis van digitalisering voor de samenleving. Diverse rapporten benadrukken dat verschillende publieke waarden onder druk staan als gevolg van digitalisering. In 2017 hadden diverse adviezen vooral betrekking op de gevolgen van digitalisering als geheel. In 2018 kwamen daar adviezen bij met aandacht voor specifieke sectoren, zoals energie, mobiliteit, zorg en media, en aandacht voor specifieke technologiegebieden, zoals AI en digitale veiligheid. Op Europees niveau vragen diverse adviesraden vooral aandacht voor AI.

4.1 Nederland

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’ (WRR, 1976).

In juni 2018 heeft het kabinet de WRR gevraagd onderzoek te doen naar de impact van AI op publieke waarden (Kamerstukken, 2017-2018, 26 643, nr 529). Verder is de WRR in 2018 een project begonnen over de zogenoemde digitale ontwrichting (grootschalige verstoringen van de digitale infrastructuur).

Eerder, in 2017, publiceerde de WRR het rapport *Weten is nog geen doen. Een realistisch perspectief op redzaamheid*. Daarin introduceert de raad, als tegenhanger van ‘denkvermogen’, het begrip ‘doenvermogen’ van burgers: de

mogelijkheid om te kunnen handelen in een bepaalde situatie. Digitale geletterdheid valt er ook onder. De WRR concludeert dat de participatiesamenleving hoge eisen stelt aan dat doenvermogen. Volgens de raad zijn er grote verschillen tussen wat van burgers wordt verwacht en wat zij daadwerkelijk aankunnen. De WRR adviseert in beleid uit te gaan van een *realistisch* perspectief van het denk- en doenvermogen van burgers. Dat kan door bij de voorbereiding van beleid te toetsen of rekening is gehouden met verschillen in doenvermogen, en bij de uitvoering van beleid vroegtijdig en persoonlijk contact met burgers om ondersteuning te bieden (WRR, 2017, p. 14-15).

In de kabinetsreactie in 2018 op *Weten is nog geen doen* onderschrijft het kabinet het advies van de WRR (Kamerstukken II 2017-2018, 34775, nr 88). Het stelt onder andere voor dat de overheid informatie aanbiedt die aansluit bij verschillende niveaus van cognitieve vermogens en doenvermogens.[99] Daarnaast zal het kabinet een doenvermogentoets invoeren bij nieuwe beleidsvorming, door het te incorporeren in de al bestaande Uitvoerings- en Handhavingstoets. Het kabinet zal ook de gedragskennis bij de departementen versterken door het Behavioural Insights Netwerk Nederland (BIN NL) van de departementen bijeen te brengen. Dat is een samenwerkingsverband van alle ministeries, gericht op de toepassing van gedragsinzichten in beleid, uitvoering, toezicht en communicatie. Ten slotte geeft het kabinet aan dat het Wetenschappelijk Onderzoek- en Documentatiecentrum van het ministerie van Justitie en Veiligheid (WODC) in 2018 van start gaat met het onderzoek *Juridische aspecten van algoritmen die zelfstandig besluiten nemen*. Daarbij zal gekeken worden naar kansen die AI kan bieden voor een tijdige signalering van mensen die door omstandigheden niet zelfredzaam zijn, om deze mensen eerder en beter te helpen (Kamerstukken II 2017-2018, 34775-VI, nr 88).

Raad van Cultuur

De Raad van Cultuur is een adviesorgaan van de regering en het parlement op het gebied van kunst, cultuur en media.

In februari 2018 publiceerde de raad het sectoradvies *Zicht op zo veel meer* (Raad van Cultuur, 2018). Daarin stonden aanbevelingen om de Nederlandse audiovisuele sector toekomstbestendig te maken. Door veranderingen in het medialandschap en de komst van grote internationale spelers, moeten Nederlandse producten steeds meer concurreren met ‘superplatforms’, zoals Netflix en YouTube. Dit verdringt Nederlandse programma-aanbieders en vermindert hun bereik. Hierdoor komen belangrijke publieke waarden, zoals verhalen vertellen die

99 TNO voerde in opdracht van het Ministerie van BZK het onderzoek *Inclusief iedereen* uit, waarbij gekeken werd naar mogelijkheden om groepen die een sterke voorkeur voor telefonisch of persoonlijk contact hebben vanwege een fysieke of cognitieve beperking of door gebrek aan kennis en ervaring en het lastig vinden om informatie- en communicatietechnologie te gebruiken beter te bedienen.

Nederland bouwen en die de Nederlandse identiteit representeren, in het gedrang. De raad benadrukt het belang van samenwerken met de superplatforms om effectief in te kunnen spelen op de technologische ontwikkelingen in het mediadomein.

Tegelijkertijd is publieke financiering voor de publieke omroep en de filmsector sterk gedaald. De raad pleit daarom voor extra investeringen in de audiovisuele sector. Hij adviseert onder andere om heffingen in te stellen voor alle eindexploitanten van betaalde en gratis offline en online audiovisuele diensten – grote buitenlandse distributieplatforms zoals bioscoopketens, kabelmaatschappijen, en betaal- en superplatforms, die niet of nauwelijks bijdragen aan de financiering van Nederlandse producties – en om het huidige Filmfonds tot een breed audiovisueel fonds te maken. Ook moet volgens de raad vermeden worden dat veel geld in de sector verdwijnt naar grote commerciële bedrijven die niet de verantwoordelijkheid nemen om Nederlandse verhalen te vertellen.

De raad stelt ten slotte voor mediawijsheid en filmeducatie meer te stimuleren, en culturele audiovisuele producten te versterken door te investeren in talentontwikkeling en door kwalitatief hoogwaardige content te stimuleren (Raad van Cultuur, 2018).

Raad voor de leefomgeving en infrastructuur
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.

Met de publicatie *Technologie op waarde schatten – een handreiking* (Rli, 2017) richt de Rli zich op de complexe effecten van technologische ontwikkelingen op onze samenleving en leefomgeving, en geeft richtlijnen hoe met technologische ontwikkelingen om te gaan.[100]

In dat rapport benoemt de RLi diverse aandachtspunten voor sturing door alle betrokken partijen, waaronder het vergroten van kennis en inzicht van technologische innovaties door verschillende partijen te laten samenwerken en kennis te delen, en te sturen op doelen. De raad adviseert de overheid hierbij een prominente rol te laten spelen om publieke waarden te beschermen. Volgens de raad vraagt het gebruik van technologie bovendien om het (her)definiëren van relaties tussen overheid, bedrijfsleven, maatschappelijke organisaties en burgers, en van nieuwe relaties. Deze veranderende relaties brengen drie kwetsbaarheden met zich mee, aldus de raad: de beschikbaarheid van vitale infrastructuren,

100 Het rapport bouwt voort op het eerdere rapport *Verkenning technologische innovaties in de leefomgeving* (Rli, 2015)

toegankelijkheid van technologie – lees: de vaardigheden van gebruikers – en controleerbaarheid van technologie (specifiek algoritmen). Ten slotte bepleit de raad vooral brede maatschappelijke discussies over keuzes die overheden, bedrijven en burgers moeten maken in het licht van deze technologische ontwikkelingen (Rli, 2017).

In zijn advies *Stroomvoorziening onder digitale spanning* (Rli 2018) analyseert de Rli de kwetsbaarheden die in het elektriciteitssysteem ontstaan door het voortgaande proces van digitalisering. Het gaat daarbij niet alleen om de dreiging van cybercriminaliteit, maar ook om de mogelijke gevolgen van softwareontwerpfouten en onvoorzien gedrag van autonome systemen die de stroomvoorziening in toenemende mate zullen reguleren. Deze kwetsbaarheden brengen volgens de Rli nieuwe risico's met zich mee voor de betrouwbaarheid van de stroomvoorziening. De Rli raadt de overheid aan de mogelijke gevolgen voor de betrouwbaarheid van de stroomvoorziening te onderkennen en onderzoeken, en 'no-regret'-maatregelen te nemen om digitale kwetsbaarheden te beperken.[101] Ook zou de overheid volgens de Rli moeten investeren in een infrastructuur voor gezamenlijke kennisvergaring, en zoeken naar Europese samenwerking om kwetsbaarheden van de gedigitaliseerde stroomvoorziening aan te pakken (Rli, 2018).

Sociaal en Cultureel Planbureau

Het Sociaal en Cultureel Planbureau (SCP) is een kennisinstelling van de overheid die beleidsrelevant wetenschappelijk onderzoek doet. Het valt formeel onder het ministerie van Volksgezondheid, Welzijn en Sport (VWS). Het SCP monitort onder andere de leefsituatie en kwaliteit van leven in Nederland, evalueert overheidsbeleid en verkent de samenleving voor toekomstig beleid.

In 2017 bracht het zijn tweejaarlijkse rapport uit over de sociale staat van Nederland. Daarin was ook aandacht voor de digitale zelfredzaamheid van burgers. Daar wordt een steeds groter beroep op gedaan, onder meer vanwege technologische ontwikkelingen en de flexibilisering van de arbeidsmarkt. Er zijn echter grote groepen mensen – bijvoorbeeld laaggeletterden of mensen met een (lichte) verstandelijke beperking – voor wie het moeilijk of zelfs onmogelijk is om zich digitaal te redden. De informatiesamenleving lijkt deze groepen mensen te vergeten, waardoor een digitale kloof ontstaat. Daarom is het volgens het SCP van belang dat de samenleving zich inspant om zo veel mogelijk burgers volwaardig mee te laten doen. Dat kan onder meer door hen te helpen de noodzakelijke (digitale) vaardigheden op te doen. Hierbij verwijst het SCP onder meer naar het WRR-rapport (2017) over het zogenoemde doenvermogen (SCP, 2017).

101 Bijvoorbeeld door preventieve maatregelen te nemen en te waarborgen dat actuele inzichten over veilig ontwerp en updaten van digitale systemen in standaarden worden vastgelegd.

Centraal Planbureau
Het Centraal Planbureau (CPB) is een onderzoeksinstituut dat economische beleidsanalyses uitvoert. Het is onderdeel van het ministerie van EZK.

In 2018 pleitte het CPB in het rapport *CPB Risicorapportage Financiële Markten 2018* (2018) voor 'cyberstresstests' bij banken, waarmee die de digitale veiligheid kunnen toetsen. Actief toezicht van De Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten op IT-systemen is daarvoor cruciaal, aldus het CPB. DNB is samen met partners al bezig met het opzetten van cyberveiligheidstests.

In 2017 publiceerde het CPB ook het rapport *Scientia potentia est: de opkomst van de makelaar voor alles* (CPB, 2017). Daarin waarschuwt het tegen de negatieve gevolgen van digitale platforms (zoekmachines, sociale platforms en onlinemarktplaatsen zoals Google, Facebook, en Amazon). Het bureau benoemt in het bijzonder het risico dat platformbedrijven misbruik maken van hun informatiepositie. Ook noemt het CPB het risico van onvoldoende prikkels voor platformbedrijven om ongewenst gedrag van hun gebruikers tegen te gaan, zoals de verspreiding van desinformatie. Het CPB schrijft dat de overheid maatregelen kan nemen om risico's bij platforms te beperken door de transparantie en aansprakelijkheid van platforms te vergroten. Daarbij moet de overheid wel oog hebben voor de vrijheid van meningsuiting en de ruimte voor innovatie. Het CPB pleit voor een vergunningenstelsel voor platforms, zodat toezichthouders grip kunnen houden op de partijen die daarop actief zijn. Andere voorstellen van het CPB zijn onder andere om platforms te verplichten schadelijke informatie te markeren of te filteren en om duidelijk te maken wanneer informatie afkomstig is van politieke partijen (CPB, 2017).

In de kabinetsreactie op het rapport *Scientia potentia est* onderschrijft het kabinet de risico's van internetplatforms die het CPB signaleert (Kamerstukken II, 2017-2018, 33009, nr 48). Het kabinet geeft aan te hechten aan de genoemde ruimte voor platforms om zich innovatief te blijven ontwikkelen. Het stelt dat voor de aanpak van de risico's vaak al instrumenten beschikbaar zijn in bestaande wet- en regelgeving. En het wil een kwalitatief goede nieuwsvoorziening in Nederland, met aandacht voor desinformatie en heimelijke beïnvloeding in Nederland (Kamerstukken II, 2017-2018, 26643, nr 508). Ook verwijst het kabinet in zijn reactie naar de aangenomen motie Heerma/Mohandis, die de regering verzoekt 'onderzoek in te stellen naar de toekomst van de onafhankelijke journalistiek in Nederland in relatie tot de verspreiding van desinformatie' (Kamerstukken II, 2016-2017, 34550 VIII, nr 82). Ten slotte verwijst de kabinetsreactie naar een Nationale

Digitaliseringsstrategie,[102] waarin aandacht zal zijn voor de risico's, transparantie en aansprakelijkheid van platforms (Kamerstukken II, 2017-2018, 33009, nr 48).

Planbureau voor de Leefomgeving
Het Planbureau voor de Leefomgeving (PBL) is een overheidsinstantie voor het maken van strategische beleidsanalyses op het gebied van milieu, natuur en ruimte. Het valt formeel onder het ministerie van Infrastructuur en Milieu (IenM), maar doet onderzoek voor meerdere departementen.

In de publicatie *Mobiliteit en elektriciteit in het digitale tijdperk. Publieke waarden onder spanning* (PBL, 2017) staat dat publieke waarden onder druk staan door digitalisering van infrastructuur. Denk aan gelijke toegang tot het openbaar vervoer; transparantie, voorzieningszekerheid en leveringszekerheid van vitale (energie)voorzieningen zoals elektriciteit; bescherming van privacy en zelfbeschikking; en democratische controle (vooral ten aanzien van intelligente systemen). Volgens het PBL kan digitalisering ertoe leiden dat bepaalde groepen, zoals laagopgeleiden en ouderen, worden uitgesloten van dienstverlening als zij niet de noodzakelijke vaardigheden hebben of geen gebruik kunnen maken van nieuwe infrastructuurdiensten.

Een ander risico volgens het PBL is de toename van de kwetsbaarheid van storingen en uitval, vooral wanneer netwerken complexer worden. Daarom bepleit het bureau dat sturing vanuit de overheid belangrijk is om te voorkomen dat een kloof ontstaat tussen burgers door verschillen in digitale geletterdheid, of maatschappelijke ontwrichting door gebrekkige beheersbaarheid van vitale (energie)voorzieningen. Ook stelt het planbureau voor dat de overheid actief met de samenleving in gesprek gaat over kernwaarden, om duidelijke kaders en doelen te stellen om publieke waarden te beschermen. Verder wijst het op de noodzaak voor passend toezicht en democratische controle met betrekking tot smart city toepassingen.

Ten slotte adviseert PBL meer te investeren in de digitale expertise van de overheid, omdat overheden meer technische kennis van de nieuwe gedigitaliseerde systemen nodig hebben, en meer kennis nodig hebben van de ethische en maatschappelijke impact van digitalisering op de samenleving (PBL, 2017).

In de kabinetsreactie onderschrijft het kabinet het advies van het PBL dat de publieke waarden als toegankelijkheid, leveringszekerheid, privacy en democratische controle onder druk komen te staan door de toenemende complexiteit van systemen (Kamerstukken II 2017-2018, 29023, nr 228). Het vindt

102 Aangekondigd tijdens de begrotingsbehandeling van EZK op 14 december 2017.

echter niet dat de digitale veiligheid van de vitale infrastructuur niet op orde is. Wel vindt het kabinet dat digitale veiligheid van toenemend belang is voor de leveringszekerheid. Op dit moment is de leveringszekerheid geborgd door de Elektriciteitswet 1998, waarbij de verantwoordelijkheid ligt bij de netbeheerder. Het kabinet geeft aan te zullen verkennen welke waarborgen noodzakelijk zijn om de leveringszekerheid van elektriciteit op peil te houden en welke lessen we kunnen leren van andere landen ten aanzien van de borging van de veiligheid van vitale infrastructuur in het kader van digitalisering. Daarnaast wordt met de implementatie van de Cybersecuritywet (zie hoofdstuk 5) geprobeerd de Europese samenwerking bij ICT-incidenten te verbeteren en de veerkracht van netwerk- en informatiesystemen van vitale diensten te versterken (Kamerstukken II 2017-2018, 29023, nr 228).

Onderwijsraad

De Onderwijsraad is een onafhankelijk adviescollege dat de regering en de Eerste en Tweede Kamer over hoofdlijnen van beleid en wetgeving op het gebied van het onderwijs adviseert. Volgens de Onderwijsraad vraagt de snel digitaliserende samenleving om onderwijs waarin plaats is voor digitale onderwijsdoelen, de inzet van digitale leermiddelen, en het gebruik van digitale toepassingen voor de organisatie van het onderwijs.

In het advies *Doordacht digitaal* (Onderwijsraad, 2017) pleit de Onderwijsraad voor het maken van doordachte onderwijskeuzes om ervoor te zorgen dat het onderwijs optimaal kan profiteren van de mogelijkheden die digitalisering biedt. De raad adviseert de rijksoverheid scholen meer te ondersteunen bij het op orde krijgen van de randvoorwaarden voor digitalisering, zoals internetveiligheid en privacy. Daarnaast pleit de raad voor een nauwere betrokkenheid van het onderwijsveld bij digitale ontwikkelingen en bij het vormgeven van innovatieve toepassingen; de digitale deskundigheid in het onderwijsveld moet volgens de raad structureel worden uitgebouwd. Dat kan door scholen zelf te laten experimenteren met ICT. Bovendien waarschuwt de raad tegen mogelijke negatieve gevolgen van veelvuldig gebruik van digitale toepassingen voor het geheugen en het concentratievermogen, en schadelijke fysieke en psychische gevolgen van veelvuldig internetgebruik, zoals ‘tabletnekken’, cyberpesten en ‘disconnectie-angst’, het gevoel iets te missen als je offline bent. De raad benadrukt ten slotte dat een brede inzet van ICT in het onderwijs niet mag leiden tot een bedreiging van een veilige pedagogische didactische omgeving waarin leerlingen zich kwetsbaar of rebels mogen opstellen zonder daar later mee geconfronteerd te worden.[103] (Onderwijsraad, 2017).

103 Bijvoorbeeld doordat bepaalde sporen achterblijven op het internet of doordat digitale data over individuele leerlingen in het onderwijssysteem blijven bestaan.

In de kabinetsreactie op het advies onderschrijft het ministerie van OCW de aanbevelingen (Kamerstukken II 2016-2017, 32034, nr 22). Het ministerie erkent onder andere het belang van een goede basisinfrastructuur. Het wil daarom regie blijven voeren met de sectororganisaties op de verdere ontwikkeling van de basisinfrastructuur. Ook onderschrijft OCW het belang van het scheiden van techniek en inhoud. Daarom heeft het onderwijs met het bedrijfsleven en OCW standaarden afgesproken voor ICT-voorzieningen. Bovendien deelt OCW de opvatting dat het borgen van privacy en beveiliging alsmaar belangrijker wordt. De staatssecretaris heeft in een eerder Kamerstuk aangegeven dat diverse hulpmiddelen al gerealiseerd zijn, zoals het social-mediaprotocol, een *quick scan privacy*, en handreikingen om ouders te informeren. Daarnaast wordt de invoering gerealiseerd van een pseudoniem voor leerlingen die digitale leermiddelen gebruiken, die tot doel heeft privacy van leerlingen beter te beschermen (Tweede Kamer, vergaderjaar 2016-2017, Aanhangsel van de Handelingen, 2075; Kamerstukken II 2016-2017, 32034, nr 22; Kamerstukken II 2016-2017, 34741, nr 2).

De Sociaal-Economische Raad

De Sociaal-Economische Raad is een adviesorgaan dat regering en parlement adviseert over de hoofdlijnen van het te voeren sociaal-economisch beleid. De SER en het kabinet gingen in 2017, ondersteund door de internationale denktank OESO, van start met het ontwikkelen van een ‘nationale skills-strategie’.[104] Ook publiceerde de SER in juni 2017 het advies *Leren en ontwikkelen tijdens de loopbaan*. Verder organiseerde de SER samen met het Rathenau Instituut twee werkconferenties over het toewerken naar een verantwoorde digitale samenleving (Rathenau Instituut & SER, 2018).[105]

Rathenau Instituut

Het Rathenau Instituut heeft het de taak om de publieke en politieke meningsvorming over wetenschap en technologie te stimuleren. Het instituut heeft de afgelopen dertig jaar de invloed van automatisering en digitalisering op allerlei domeinen van de samenleving in kaart gebracht. Zo heeft het laten zien hoe ingrijpend robotisering en digitalisering zijn voor de werkgelegenheid, digitale veiligheid en gezondheidszorg, en de invloed van *big data* en van technologieën als *augmented reality* en het IoT op mensenrechten, patiëntenrechten en consumentenrechten, en wat ervoor nodig is om die te borgen.

---

104 Zie: https://www.ser.nl/nl/actueel/werkprogramma/skills-strategie.aspx en OESO (2017) OECD Skills Strategy Diagnostic Report. Netherlands. Paris: OESO.

105 Zie: https://www.rathenau.nl/nl/digitale-samenleving/acties-voor-een-verantwoorde-digitale-samenleving. Dit naar aanleiding van het rapport *Opwaarderen* van het Rathenau Instituut, en de SER-verkenning *Mens en Technologie: samen aan het werk* (SER 2016), waarin de gevolgen van digitalisering en robotisering voor de arbeidsmarkt, de organisatie van werk en arbeidsverhoudingen worden geschetst.

De focus in de periode 2017-2018 lag op het borgen van publieke waarden in de digitale samenleving.[106] Op 9 maart 2018 verscheen de kabinetsreactie op het rapport *Opwaarderen* en het rapport *Human rights in the robot age* (Kamerstukken II, 2017-2018, 26643, nr 529). Deze kabinetsreactie bespreken we in hoofdstuk 5.

Het rapport *Human rights in the robot age* schreef het Rathenau Instituut in 2017 op verzoek van de Parlementaire Assemblee van de Raad van Europe (PACE) (Van Est & Gerritsen, 2017).[107] Daarin pleiten we voor twee nieuwe mensenrechten: het recht om niet gemeten, geanalyseerd of beïnvloed te worden, en het recht op betekenisvol menselijk contact. Het rapport kijkt naar het gebruik van robots, AI en *virtual* en *augmented reality*, en de effecten daarvan op mensenrechten. Het rapport dient als achtergrond voor de door PACE ingestelde rapporteur Mr Le Déaut. PACE heeft op basis van het onderzoek op 28 april 2017 de resolutie *Technological convergence, artificial intelligence and human rights* aangenomen en de Raad opgeroepen te kijken hoe intelligente voorwerpen mensenrechten uitdagen. Op 19 oktober 2017 heeft de Commissie van Ministers van de Raad van Europa de aanbevelingen in de resolutie van PACE aangenomen (zie hoofdstuk over grond- en mensenrechten).

Met het rapport *Eerlijk delen. Waarborgen van publieke belangen in de deeleconomie en de kluseconomie* (2017)[108] adviseert het Rathenau Instituut dat maatschappelijke belangen in de deeleconomie beter moeten worden beschermd. De opkomst van online deelplatformen zet publieke waarden onder druk, zoals consumentenbescherming, openbare orde en privacy. Het rapport doet een aantal concrete aanbevelingen. Ten eerste zou de overheid de juridische status van deel- en klusplatformen moeten verhelderen. Verder zou de overheid een derde, vertrouwde partij kunnen aanstellen voor het toezicht op een platform, op een manier die de privacy van deelnemers waarborgt. Tot slot moet worden gestimuleerd dat beoordelingen betrouwbaar en mee te nemen zijn. Naar aanleiding van het rapport heeft de Tweede Kamer er een zogenoemd dertigledendebat over gehouden (Handelingen TK 2017-2018, 9), en verscheen in januari 2018 de kabinetsreactie (Kamerstukken II, 2017-2018, 33009, nr 47). Daarin geeft het kabinet aan, ernaar te streven om de negatieve effecten van de deeleconomie te voorkomen of te beperken, en de positieve effecten ervan te stimuleren.

106 Zie werkprogramma voor 2017-2018: https://www.rathenau.nl/nl/publicatie/werkprogramma-2017-2018
107 Zie: https://www.rathenau.nl/nl/digitale-samenleving/mensenrechten-het-robottijdperk
108 Zie: https://www.rathenau.nl/nl/digitale-samenleving/eerlijk-delen

Het Rathenau Instituut stelt met het rapport *Een nooit gelopen race* (Munnichs et al. 2017)[109] dat het versterken van de digitale veiligheid in Nederland meer prioriteit moet krijgen. We deden dit onderzoek op verzoek van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en de inlichtingendienst AIVD. Het rapport maakt duidelijk dat Nederland, als een van de meest ICT-intensieve economieën ter wereld, een aantrekkelijk doelwit is voor cybercriminelen, cyberspionnen en hackers. De ontwikkeling van IoT versterkt bestaande kwetsbaarheden. Cyberdreigingen ondermijnen volgens het rapport het innovatie- en concurrentievermogen van het Nederlandse bedrijfsleven en het vertrouwen in de digitale samenleving. Het Rathenau Instituut pleit daarom onder andere voor jaarlijkse hacktests en een onafhankelijk kennis- en adviescentrum voor mkb-bedrijven. Het beveelt aan te onderzoeken of de bestaande aansprakelijkheidswetgeving voldoende is voor ICT-producten en –diensten. Toezichthouders als de ACM en het Agentschap Telecom zouden bovendien krachtiger moeten optreden tegen het op de markt brengen van onveilige digitale producten.

Op verzoek van het Europees Parlement deden we ook onderzoek naar digitale burgerparticipatie. We publiceerden het rapport *Online meebeslissen - Lessen uit onderzoek naar digitale burgerparticipatie voor het Europees Parlement* (Korthagen & Van Keulen, 2017).[110] Daaruit blijkt dat digitale participatie de democratie kan versterken. Op basis van vele Europese casestudies zijn zes voorwaarden opgesteld voor de overheid om te komen tot succesvolle digitale participatietrajecten. Zo is het van belang dat het proces aan een concrete agenda of besluit wordt verbonden, helder over het proces en doel wordt gecommuniceerd, feedback wordt gegeven aan de deelnemers ten aanzien van hun bijdragen, en meer wordt gedaan dan het verzamelen van handtekeningen. Ook is een effectieve communicatie- en mobiliteitsstrategie bestaande uit meerdere instrumenten op maat cruciaal om verschillende doelgroepen te bereiken. Daarnaast is digitale burgerbetrokkenheid een leerproces en moet het daarom herhaald en verbeterd blijven worden.

In mei 2018 verscheen het rapport *Digitalisering van het nieuws* (Van Keulen et al., 2018).[111] Het Rathenau Instituut stelt daarin dat Nederland tot op heden geen grote nadelen heeft ondervonden van de verspreiding van desinformatie. Er zijn weinig Nederlanders die hun nieuws alleen krijgen via sociale media of zoekmachines. Ook ervaren Nederlanders een ruime mate van diversiteit in berichtgeving. Toch kunnen de vitale functies van de nieuwsvoorziening voor het Nederlandse publieke en politieke debat alsnog onder druk komen te staan, door technologische

109 Zie: https://www.rathenau.nl/nl/digitale-samenleving/een-nooit-gelopen-race
110 Zie: https://www.rathenau.nl/nl/kennis-voor-beleid/online-meebeslissen
111 Zie: https://www.rathenau.nl/nl/digitale-samenleving/digitalisering-van-het-nieuws

ontwikkelingen op het gebied van manipulatie van audio en video, het 'levensecht' maken van automatische computeraccounts (*social bots*) waardoor deze lastiger te detecteren zijn, en verdere personalisatie van nieuwsstromen. Daarom moet Nederland zich voorbereiden op de toekomst en onder meer investeren in 'technologisch burgerschap' door meer inzicht te verwerven in hoe technologie werkt, opdat ze er kritisch over kunnen nadenken en begrijpen wat de betekenis ervan is voor leefwereld en maatschappij.

In mei 2018 verscheen ook het rapport *Robotisering en automatisering op de werkvloer* (Freese et al., 2018).[112] Daarin laten we zien voor welke keuzes bedrijven staan bij de introductie van nieuwe digitale technologie. Het biedt concrete handvatten voor bedrijven die zicht willen krijgen op de overwegingen die van belang zijn bij de introductie van nieuwe technologie op de werkvloer. De kern daarvan is: een gedegen voorbereiding is essentieel voor het laten slagen van digitale innovatie op de werkvloer. De aanbevelingen om die voorbereiding vorm te geven zijn: onderkennen dat nieuwe digitale technologie vraagt om nieuwe werkprocessen, anticiperen op nieuwe verdienmodellen, oog hebben voor nieuwe kwetsbaarheden in het bedrijfsproces, en medewerkers betrekken bij de introductie, en concrete handvatten voor bedrijven.

Ten slotte publiceerden we op verzoek van de Vereniging Nederlandse Gemeenten (VNG) het rapport *Waardevol Digitaliseren* (Van Est et al. 2018),[113] waarin de kansen en risico's van digitalisering voor lokaal bestuur besproken worden. Een belangrijke boodschap is dat innoveren en digitaliseren niet alleen draaien om technologische en economische innovatie, maar ook om sociale en juridische inbedding. Het rapport komt met tien zienswijzen die het handelen van lokale bestuurders richting kunnen geven op dit terrein.

Cyber Security Raad

De Cyber Security Raad is een nationaal en onafhankelijk adviesorgaan van het kabinet en is samengesteld uit vertegenwoordigers van publieke en private organisaties en de wetenschap. De CSR zet zich op strategisch niveau in om de digitale veiligheid in Nederland te verhogen.[114]

Met het rapport *Ieder bedrijf heeft digitale zorgplichten* (CSR, 2017a) biedt de CSR een handreiking met een overzicht van de belangrijkste juridische zorgplichten op het gebied van digitale veiligheid en de belangrijkste handvatten. De raad bespreekt daarin de verantwoordelijkheid van de verschillende partijen met betrekking tot privacy en veiligheid.

112 Zie: https://www.rathenau.nl/nl/digitale-samenleving/robotisering-en-automatisering-op-de-werkvloer
113 Zie: https://www.rathenau.nl/nl/digitale-samenleving/waardevol-digitaliseren
114 Zie: https://www.cybersecurityraad.nl/

In het rapport *Naar een veilig verbonden digitale samenleving* (CSR, 2017c) benadrukt de raad dat de huidige IoT-toepassingen slecht beveiligd zijn en publieke waarden als veiligheid en vrijheid in het gedrang komen. De raad adviseert de invoering van een label-systeem waarbij stickers en certificaten ofwel keurmerken op verpakkingen van IoT-producten, informatie bieden aan consumenten over de beveiliging van het product. De raad pleit ook voor een voorlichtingscampagne en het opstellen van een handleiding over label-systeem. Daarnaast stelt de raad voor om veiligheidseisen aan leveranciers te stellen en meer toezicht op fabrikanten in te voeren. De raad pleit bovendien voor een onafhankelijke monitor die informatie beschikbaar maakt over welke fabrikanten en leveranciers hun producten onvoldoende beveiligen.

Met het rapport *Naar een landelijk dekkend stelsel van Informatieknooppunten. Advies inzake informatie-uitwisseling met betrekking tot cybersecurity en cybercrime* (CSR, 2017b) benadrukte de CSR dat het delen en analyseren van informatie het mogelijk maakt om de digitale veiligheid van organisaties te vergroten, en organisaties weerbaarder te maken tegen cyberincidenten en/of de schade ervan te beperken. De raad stelt voor om de informatie-uitwisseling in Nederland te verbeteren door de invoering van een landelijk dekkend stelsel van informatieknooppunten, de invoering van randvoorwaarden voor succesvolle informatie-uitwisseling via de informatieknooppunten, en het vergroten van het inzicht in cyberdreigingen door het stimuleren van het doen van meldingen en het versterken van de publiek-private samenwerking op dit terrein.

Ten slotte onderstreept de CSR in het rapport *Naar een open, veilig en welvarend digitaal Nederland. Advies inzake de Nederlandse Cybersecurity Agenda (NCSA)* (CSR, 2018) het belang van een gedegen visie op het beschermen van kernwaarden in een omgeving waarin we als land voor onze cybersecurity vaak afhankelijk zijn van machtige, internationale bedrijven. Volgens de CSR staat Nederland voor de vraag hoe we kernwaarden die belangrijk zijn voor een open, veilige en welvarende digitale samenleving kunnen borgen. De CSR adviseert een integrale aanpak waarbij het kabinet, de overheid, het bedrijfsleven en de overheid betrokken worden. De CSR wil dat de NCSA de focus legt op de volgende drie onderwerpen: inventarisatie en besluitvorming fundamentele vraagstukken, slagvaardige en samenhangende implementatie van de NCSA, en structureel investeren in cybersecurity.

Raad voor Volksgezondheid en Samenleving

De Raad voor Volksgezondheid en Samenleving (RVS) is een onafhankelijk adviesorgaan voor de regering en de beide Kamers van de Staten-Generaal. De RVS heeft tot taak strategische adviezen te geven over het te voeren beleid,

waarbij alle aspecten die van invloed zijn op de gezondheid en het functioneren van burgers in de samenleving worden betrokken.[115] De RVS bereidt binnen het thema 'De belofte van wetenschap en technologie' een advies voor als vervolg op de conferentie 'Mens en Machine: wie maakt wie?' Dit advies onderzoekt veranderingen in de zorg door gebruik van medische expertsystemen, en hoe keuzevrijheid en regie geborgd kunnen worden. De publicatie wordt in de tweede helft van 2018 verwacht.

Raad voor het Openbaar Bestuur

De Raad voor het Openbaar Bestuur (ROB) is een onafhankelijk adviesorgaan dat adviseert over de inrichting en het functioneren van het openbaar bestuur en de beginselen van democratie en rechtsstaat. Op verzoek van de minister van BZK onderzoekt de raad de kansen en risico's van digitalisering voor de democratie (Kamerstukken II, 2017-2018, 34775, nr 52). Hierbij kijkt de raad naar de positieve en negatieve gevolgen van platforms en digitalisering voor het democratisch debat, en de mogelijke rollen van het bedrijfsleven en de overheid. Het advies wordt begin 2019 verwacht.

Tabel 9 Overzicht activiteiten adviesraden Nederland digitalisering en publieke waarden, op hoofdlijnen (periode 1 januari 2017 - 30 juni 2018)

Wie/wat	Technologie	Issue	Actie
Wetenschappelijke Raad voor het Regeringsbeleid			
Adviesaanvraag AI	AI	Publieke waarden	Multi-disciplinair onderzoek naar impact AI op publieke waarden
Digitale ontwrichting	Digitalisering	Digitale veiligheid	Lopend
Weten is nog geen doen. Een realistisch perspectief op redzaamheid	o.a. digitalisering	Autonomie	Overheid moet in haar beleid uitgaan van een realistisch burgerperspectief
Raad van Cultuur			
Advies over de audiovisuele sector	Digitalisering, platforms	Waarborgen publieke waarden, waaronder Nederlandse verhalen in de audiovisuele sector	Advies voor kleinere platforms om samen te werken met superplatforms om verdringing tegen te gaan, en om heffingen voor eindexploitanten in te voeren om de financiële circulariteit binnen de sector te bevorderen

115 Zie: https://www.raadrvs.nl/raad/over-rvs

Raad voor de leefomgeving en infrastructuur			
Technologie op waarde schatten – een handreiking	Digitalisering, autonome voertuigen, deeleconomie	Veiligheid, autonomie, controle over technologie	Advies voor evenwicht tussen wendbaarheid en stabiliteit, nieuwe relaties tussen partijen definiëren, nieuwe kwetsbaarheden onderkennen, en oog voor publieke waarden
Stroomvoorziening onder digitale spanning	Digitalisering, AI	Digitale veiligheid	De overheid moet digitale kwetsbaarheden van de stroomvoorziening beperken
Sociaal en Cultureel Planbureau			
De sociale staat van Nederland 2017	O.a. digitalisering	Autonomie (redzaamheid, digitale vaardigheden)	Overheid speelt een grote rol in het verschaffen van benodigde hulpbronnen
Centraal Planbureau			
Scientia potentia est: de opkomst van de makelaar voor alles	Digitalisering, platforms	Privacy, veiligheid, autonomie, democratie	Overheid moet maatregelen treffen om risico's van het doorgeven van misleidende informatie door platforms te beperken
Planbureau voor de Leefomgeving			
Mobiliteit en elektriciteit in het digitale tijdperk, Publieke waarden onder spanning	Digitalisering	Veiligheid, controle over technologie, machtsverhoudin-gen	Meer overheidsregie nodig om publieke kernwaarden te waarborgen
Onderwijsraad			
Doordacht Digitaal	Digitalisering in het onderwijs	Privacy, veiligheid, autonomie (vaardigheden)	Onderwijs moet nauwer betrokken worden bij en meegaan met digitale ontwikkelingen
Sociaal-Economische Raad			
Leren en ontwikkelen	Oa. digitalisering	Inclusieve arbeidsmarkt	

Rathenau Instituut			
Human rights in the robot age: challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality	Robotica, AI, *virtual* en *augmented reality*	Privacy, veiligheid, autonomie, controle over technologie, menselijke waardigheid, machtsverhoudingen	Pleidooi voor een nieuw Europees verdrag met twee nieuwe mensenrechten: het recht om niet gemeten, geanalyseerd of beïnvloed te worden, en het recht op betekenisvol menselijk contact
Eerlijk delen. Waarborgen van publieke belangen in de deeleconomie en de kluseconomie	Platformen	Privacy, veiligheid, autonomie, machtsverhoudingen	Advies met betrekking tot de deeleconomie waarbinnen maatschappelijke belangen beter beschermd dienen te worden
Opwaarderen. Borgen van publieke waarden in de digitale samenleving.	Digitalisering	7 publieke waarden (zie tabel 2)	De overheid, de toezichthouders, het bedrijfsleven en de samenleving zijn onvoldoende voorbereid op nieuwe ethische en maatschappelijke vragen
Regels voor het digitale mensenpark	Digitalisering	Privacy, autonomie, controle over technologie, rechtvaardigheid, menselijke waardigheid	In het tijdperk van technologische convergentie en *big data* is een bewuste politiek van ‘telen’ (door kiembaanmodificatie) en ‘temmen’ van mensen (door persuasieve technologie) noodzakelijk.
Een nooit gelopen race	Digitalisering, IoT	Veiligheid	Het versterken van digitale veiligheid moet in Nederland meer prioriteit krijgen
Digitale democratie	Digitalisering	Transparantie, inclusie, democratie	Digitale participatie kan de democratie versterken
Digitalisering van het nieuws	Digitalisering, sociale media, platformen, persuasieve technologie	Democratische waarden, desinformatie	De vitale functies van de nieuwsvoorziening voor het Nederlandse publieke en politieke debat onder druk kunnen komen te staan
Waardevol digitaliseren	Digitalisering	Publieke waarden	In kaart brengen van de kansen en risico’s van digitale innovaties op het niveau van het lokale bestuur

Cyber Security Raad			
Ieder bedrijf heeft digitale zorgplichten	Digitalisering, IoT	Digitale veiligheid, verantwoordelijkheid	Verantwoordelijkheid op het gebied van digitale veiligheid uitgelicht
Naar een veilig verbonden digitale samenleving	Digitalisering, IoT	Digitale veiligheid	Advies inzake de digitale veiligheid van het IoT
Naar een landelijk dekkend stelsel van Informatieknoop-punten	Digitalisering, IoT	Digitale veiligheid	Advies over informatie-uitwisseling met betrekking tot digitale veiligheid en cyberdreigingen
Naar een open, veilig en welvarend digitaal Nederland. Advies NCSA	Digitalisering, IoT	Digitale veiligheid	Advies hoe open, veilige en welvarende digitale samenleving te waarborgen bij toenemende afhankelijkheid buitenlandse techbedrijven
Raad voor Volksgezondheid en Samenleving			
Advies naar aanleiding van conferentie ‘Mens en Machine: wie maakt wie?’	Digitalisering	Vrijheid, controle	Waarborgen keuzevrijheid en regie in de zorg
Raad voor het Openbaar Bestuur			
Advies over de invloed van digitale platformen op het democratisch proces.	Digitalisering, platformen, persuasieve technologie	Democratische waarden	Advies beschrijft de mogelijkheden en risico’s van digitalisering voor de democratie.

Bron: Rathenau Instituut

4.2 Internationale ontwikkelingen

Organisatie voor Economische Samenwerking en Ontwikkelingen
De Organisatie voor Economische Samenwerking en Ontwikkelingen (OESO, of OECD) is een samenwerkingsverband van 35 landen en heeft als doel om beleid te bevorderen dat is gericht op het economische en sociale welzijn van mensen over de hele wereld. De OESO organiseert veel activiteiten op het gebied van digitalisering. Zo is er een Directorate For Science Technology and Innovation, en een alomvattend *Going Digital*-project om sterke en inclusieve groei van de digitale revolutie te stimuleren, en zijn er veel fora en conferenties georganiseerd op het

gebied van digitalisering. Onderwerpen zijn bijvoorbeeld AI; de digitale economie, veiligheid en privacy; en de digitale overheid, transparantie en inclusie.[116]

In maart 2018 verscheen een rapport over de uitdagingen op het gebied van belasting heffen die door digitalisering ontstaan. In het rapport stelt de OESO voor technologiebedrijven zwaarder te belasten door bedrijven in een lidstaat ook belasting te laten betalen als ze daar 'digitaal aanwezig' zijn, om te zorgen voor een gelijke grondslag voor winstbelasting in de hele EU (OESO, 2018).

Europees Economisch en Sociaal Comité
Het Europees Economisch en Sociaal Comité (EESC) is een EU-adviesorgaan dat bestaat uit vertegenwoordigers van werkgevers- en werknemersorganisaties en andere belangengroepen. Het adviseert de Europese Commissie, de Raad van de EU en het Europees Parlement over EU-aangelegenheden en fungeert daarmee als brug tussen de EU-besluitvormingsinstanties en de burgers.[117]

In 2017 heeft het EESC een initiatiefadvies geschreven over de maatschappelijke en ethische impact van AI. In het advies signaleert het EESC elf domeinen waar AI zorgt voor uitdagingen en waar actie nodig is, namelijk: ethiek; veiligheid; privacy; transparantie en verklaarbaarheid; arbeid; educatie en vaardigheden; (on)gelijkheid en inclusie; wet- en regelgeving; bestuur en democratie; oorlogsvoering; en superintelligentie (Muller, 2017).

Het EESC bepleit de vaststelling van supranationale beleidskamers rondom AI, omdat de impact van AI zich niet beperkt tot het nationaal of Europees niveau maar grensoverschrijdend is. Daarnaast beveelt het EESC aan dat de Europese Unie internationaal een voortrekkersrol inneemt bij het vaststellen van wereldwijde kaders voor beleid voor AI die in lijn zijn met de Europese waarden en fundamentele rechten. Ook pleit het EESC voor een ethische code voor de ontwikkeling en het gebruik van AI die de waarden van menselijke waardigheid, integriteit, vrijheid, privacy, culturele- en genderdiversiteit, en de fundamentele mensenrechten waarborgen. Ten slotte stelt het EESC voor Europees verantwoorde AI-systemen te ontwikkelen die voorzien zijn van Europese AI-certificering en labels, en ethische waarden als veiligheid en transparantie waarborgen.

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 wetenschap en nieuwe technologieën. De EGE is een onafhankelijke

116 Zie: http://www.oecd.org/going-digital/project/
117 Zie: https://europa.eu/european-union/about-eu/institutions-bodies/european-economic-social-committee_nl

internationale expertgroep van de voorzitter van de Europese Commissie, en is en de centrale spil in het netwerk van nationale ethiekraden uit verschillende EU-landen.[118]

In maart 2018 heeft de EGE het rapport *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems* uitgebracht, waarin de EGE de urgentie benadrukt van een internationaal erkend ethisch raamwerk voor het design, de productie, het gebruik en de governance omtrent AI, robots en autonome systemen. De EGE vraagt daarom om een brede en systematische publieke betrokkenheid en beraad ten aanzien van de ethiek rondom AI, robotica en autonome technologie in relatie tot publieke waarden. Zo stelt de EGE een aantal basisprincipes en democratische waarden op als eerste stap richting ethische richtlijnen: menselijke waardigheid, autonomie, verantwoordelijkheid, rechtvaardigheid, gelijkheid en solidariteit, democratie, accountability, veiligheid en integriteit, databescherming en privacy, en duurzaamheid. De EGE bepleit vervolgens dat een proces moet worden gestart om een internationaal erkend ethisch en juridisch raamwerk op te stellen.

Naar aanleiding van het rapport heeft de Europese Commissie een expertgroep opgericht die zich richt op AI-ethiek. Die zal richtlijnen voor ethisch gebruik van AI opstellen, voortbouwend op het rapport van de EGE en de waarden die daarin worden beschreven.

European Union Agency for Fundamental Rights
Het Europese agentschap voor fundamentele rechten (FRA) is een EU-organisatie die de Europese Commissie ondersteunt en voorziet van expertise op het gebied van fundamentele rechten. Een van de onderwerpen in het werkprogramma is de informatiesamenleving, met aandacht voor respect voor het privéleven en de bescherming van persoonsgegevens.

In mei 2018 verscheen een rapport over *big data* en discriminatie bij door data ondersteunde besluitvorming (FRA, 2018). Het rapport geeft aan hoe discriminatie kan optreden bij het gebruik van *big data*, algoritmen en AI en stelt diverse oplossingen voor om het risico van discriminatie te verminderen. De FRA is ook lid van de Europese High Level Expert Group on Artificial Intelligence (zie hoofdstuk 5). In 2019 zal de FRA onderzoek doen naar de implicaties van AI en *big data* voor fundamentele rechten.

European Political Strategy Centre
Het Europees Centrum voor Politieke Strategie (EPSC), voorheen het Bureau of European Policy Advisers (BEPA), is de interne denktank van de Europese

118 Zie ec.europa.eu/research/ege/index.cfm

Commissie, en werd opgericht in 2014 door Commissievoorzitter Jean-Claude Juncker.

In maart 2018 heeft de EPSC het paper *The Age of Artificial Intelligence. Towards a European Strategy for Human-Centric Machines* uitgebracht waarin onder andere gekeken wordt naar de ethische uitdagingen die AI met zich meebrengt (EPSC, 2018). In het rapport pleit het EPSC voor een AI-strategie en regulerende normen en richtlijnen om de ethische ontwikkeling van AI te waarborgen waarbij de mens centraal wordt gesteld en er aandacht is voor aansprakelijkheid.[119]

Tabel 10 Activiteiten binnen het politiek-bestuurlijk domein op het gebied van agendavorming, op hoofdlijnen (periode 1 januari 2017 - 30 juni 2018)

Wie/wat	Technologie	Issue	Actie
European Group on Ethics in Science and New Technologies			
Ethics of Artificial Intelligence	AI	Privacy, veiligheid, democratie, autonomie, controle over technologie, menselijke waardigheid	Internationaal ethisch en juridisch raamwerk voor ethische omgang met AI
Organisatie voor Economische Samenwerking en Ontwikkelingen (OESO, of OECD)			
Going Digital	Digitalisering, AI, platformen	Privacy, veiligheid, rechtvaardigheid, Inclusie, machtsverhoudingen	Ontwikkelen van beleid voor inclusieve groei, duurzaamheid en welzijn
Belasting uitdagingen door digitalisering	Digitalisering, platformen	Machtsverhoudingen	Voorstel technologiebedrijven gelijke winstbelasting in EU
Europees Economisch en Sociaal Comité			
AI	AI	Privacy, veiligheid, controle over technologie, autonomie, menselijke waardigheid, inclusie, democratie	O.a. Maatschappelijk debat omtrent AI vormgeven, ontwikkeling ethische code

119 Ook het Institute of Electrical and Electronic Engineers (IEEE) heeft in 2016 het Global Initiative on Ethics of Autonomous and Intelligent Systems opgericht om beleidsrichtlijnen op te stellen om ethische implementaties van AI te bevorderen.

European Union Agency for Fundamental Rights			
Thema Informatie-maatschappij	*Big data*	Beschermen grondrechten, privacy, gegevensbescher-ming, discriminatie	Identificatie uitdagingen en oplossingen met betrekking tot informatie-maatschappij
Rapport *Big data*: Discriminatie	*Big data* en algoritmen, AI	Rechtvaardigheid, controle over technologie	Identificatie uitdagingen en oplossingen betreffende *big data*
European Political Strategy Centre			
Uitdagingen AI	AI	Waarborgen van de ontwikkeling van AI waarin de mens centraal staat	AI-strategie en regulerende normen en richtlijnen

Bron: Rathenau Instituut

4.3 Conclusie

Aandacht voor digitalisering en bescherming publieke waarden
Ten opzichte van *Opwaarderen* zien we dat er meer adviesraden zijn die zich buigen over digitalisering en daaraan gerelateerde ethische en maatschappelijke kwesties. De rapporten benadrukken dat publieke waarden onder druk staan als gevolg van digitalisering. Er was daarbij in 2017 in Nederland meer aandacht voor digitalisering als geheel: diverse adviezen richtten zich niet zozeer op specifieke technologische praktijken of sectoren, maar keken naar de invloed van digitalisering, en technologische ontwikkelingen op de samenleving als geheel.

Vanaf 2018 zien we vanuit de adviesraden echter ook aandacht voor specifieke sectoren, zoals energie, mobiliteit en zorg en media, en voor specifieke technologiegebieden, zoals AI en digitale veiligheid. Op internationaal niveau (Europa) vragen adviesraden vooral aandacht voor AI.

Meer regie voor de overheid en meer dialoog
De adviesraden bepleiten in hun rapporten dat de overheid meer sturing en regie op zich neemt. Zowel met betrekking tot digitale veiligheid als binnen het onderwijs en op het niveau van de burger zien we de vraag naar een andere rol van de overheid, omdat het onderwijs en de burgers het niet alleen (aan)kunnen. De overheid wordt verondersteld meer te interveniëren om potentiële negatieve gevolgen van technologische ontwikkelingen op de samenleving in te perken.

Ook benadrukken de adviesraden het belang om in gesprek te gaan met de samenleving (bedrijfsleven, maatschappelijke organisaties en burgers) om nieuwe kaders vast te stellen.

Aandacht voor de zelfredzaamheid van burgers
In Nederland is een nieuw thema de grenzen aan de zelfredzaamheid van burgers. Diverse adviesraden vragen aandacht voor de druk die toenemende digitalisering en de overheid leggen op burgers. Daardoor kunnen diverse groepen burgers in de problemen komen –en niet alleen kleine kwetsbare groepen zoals ouderen, laaggeletterden of mensen met een beperking. Adviesraden vragen om een nieuwe rol van de overheid en een overheid die meer rekening houdt met de zogenoemde doenvermogens van burgers.

5 Politiek en bestuur: beleidsvorming en -bepaling

In de fase van beleidsvorming en -bepaling vindt de vertaling plaats van de beleidsvoorbereidende rapporten en adviezen naar visies, beleid, regelgeving, en de politieke accordering daarvan. We kijken in dit hoofdstuk naar de actoren die institutioneel verantwoordelijk zijn voor beleid en politieke besluitvorming: het kabinet, de ministeries, en het parlement. We bespreken hier de meest relevante beleidsdocumenten met het oog op ethische en maatschappelijke digitaliseringsvraagstukken van de ministeries van Binnenlandse Zaken en Koninkrijksrelaties (BZK), Economische Zaken en Klimaat (EZK), Justitie en Veiligheid (JenV), Onderwijs, Cultuur en Wetenschap (OCW) en Buitenlandse Zaken (BZ).

Met het aantreden van het nieuwe kabinet zijn er begin 2018 diverse nationale agenda's aangekondigd, waaronder in juni 2018 de overkoepelende nationale digitaliseringsagenda. Er is onder meer aandacht voor privacy, digitale veiligheid, platformen, consumentenrechten, vaardigheden en grondrechten en ethiek. Privacy en digitale veiligheid staan al geruime tijd op de beleidsagenda in Nederland. In de periode 2017-2018 zijn concrete beleidsmaatregelen aangekondigd, bijvoorbeeld de oprichting van het Digital Trust Center voor het MKB en het voornemen om certificering voor bepaalde IoT-producten te verplichten.

Andere maatschappelijke en ethische kwesties, zoals controle over algoritmen, of effecten van geautomatiseerde besluitvorming, zijn opnieuw op de agenda gekomen. Hier is het kabinet zich aan het oriënteren hoe die kwesties te vertalen zijn naar concrete beleidsmaatregelen.

Voor andere onderwerpen kijkt het kabinet naar Europa. De Europese Commissie moderniseert namelijk momenteel diverse regelgevende kaders of formuleert nieuwe kaders, o.a. op het vlak van gegevensbescherming, ePrivacy, audiovisuele en mediadiensten, auteursrecht, consumentenrechten en cybersecurity.

Het Nederlandse parlement heeft aandacht voor privacy en digitale veiligheid, en voor nieuwe kwesties, zoals inzicht in algoritmen, rechtvaardigheid en discriminatie door algoritmen, de verspreiding van desinformatie en de positie van deel- en klusplatformen.

5.1 Kabinet en ministeries

Nationale Digitaliseringsagenda
Maatschappelijke en ethische aspecten van digitalisering komen op verschillende manieren terug in de ambities van het kabinet. In juni 2018 publiceerde het ministerie van Economische Zaken en Klimaat de 'Nederlandse Digitaliseringsstrategie', in samenwerking met het ministerie van Binnenlandse Zaken en het ministerie van Justitie en Veiligheid (EZK 2018a). Deze strategie bevat een overkoepelende visie om de uitgangspunten van het kabinet te realiseren.

In verschillende afzonderlijke agenda's worden diverse punten nader uitgewerkt, zoals de Nationale Cyber Security Agenda en de Agenda Digitale Overheid; deze bespreken we hieronder bij de afzonderlijke ministeries). De strategie spreekt over een 'digitale transformatie' waar het kabinet en de samenleving voor staan. In de strategie formuleert het kabinet drie ambities:
1. vooroplopen en kansen benutten;
2. iedereen doet mee en we werken samen; en
3. vertrouwen in de digitale toekomst.

Het kabinet heeft in de strategie aandacht voor onderzoek en innovatie, de toekomst van werk, nieuwe vaardigheden en digitale geletterdheid, een concurrerende, eerlijke en transparante digitale economie, consumentenrechten, digitale veiligheid en privacy, en grondrechten en ethiek in een digitaal tijdperk (met onder andere aandacht voor de effecten van geautomatiseerde besluitvorming). Zie voor een nadere bespreking van de strategie het ministerie van EZK in paragraaf 5.1.2.

5.1.1 Ministerie van BZK

Het ministerie van BZK houdt zich op verschillende manieren bezig met de ethisch-maatschappelijke aspecten van digitalisering, voor de overheid zelf, en in zijn contact met burgers en ondernemers. Belangrijke thema's in de periode 2017-2018 waren onder andere de digitale overheid, grondrechten, digitale vaardigheden, slimme steden, desinformatie, privacy en digitale veiligheid.

Digitale overheid
In juli 2018 bracht het ministerie de Agenda Digitale Overheid uit, 'NL DIGIbeter' (BZK 2018a). Daarmee valt deze agenda buiten onze onderzoeksperiode, maar gezien de overkoepelende functie van deze agenda, hebben we het stuk hier opgenomen. De agenda maakt deel uit van de Nederlandse Digitaliseringsstrategie.

De agenda Digitale Overheid richt zich op de overheid en het contact met burgers en ondernemers. Centraal staan 'het benutten van kansen en het borgen van rechten' (BZK 2018a). De agenda bevat vijf lijnen:

1. investeren in innovatie;
2. beschermen van grondrechten en publieke waarden;
3. toegankelijk, begrijpelijk en voor iedereen;
4. dienstverlening maken we persoonlijk; en
5. klaar voor de toekomst.

In juni 2018 verscheen ook het wetsvoorstel Digitale Overheid om de digitale dienstverlening aan burgers en ondernemers te verbeteren (BZK, 2018b). De wet is erop gericht te regelen dat Nederlandse burgers en bedrijven veilig en betrouwbaar kunnen inloggen bij de (semi-)overheid, met elektronische identificatiemiddelen die betrouwbaarder zijn dan DigiD.[120] Daarop vooruitlopend verscheen in januari 2018 het Digiprogramma 2018 'Digitalisering met vertrouwen', over de ontwikkeling van de Generieke Digitale Infrastructuur (GDI) (BZK, 2018b).[121]

Digitalisering en grondrechten

In maart 2018 verscheen de kabinetsreactie op de rapporten van het Rathenau Instituut *Opwaarderen* en *Human rights in the robot age* ((Kamerstukken II, 2017-2018, 26643, nr 529). Daarin zet het kabinet uiteen welke kaders ter borging van publieke waarden en mensenrechten in de digitale samenleving gelden en welke initiatieven worden genomen (Kamerstukken II, 2017-2018, 26643, nr 529):

1. Het kabinet onderkent de impact van de nieuwe digitaliseringsgolf op publieke waarden en mensenrechten. Ook geeft het aan concrete beleidsinstrumenten in te zetten om publieke waarden en mensenrechten te borgen en zal hetdit beleid voortzetten en waar nodig intensiveren.
2. Het kabinet bespreekt het toezicht op de borging van publieke waarden en mensenrechten, en diverse dialogen over nieuwe ethische vraagstukken.
3. Het kabinet zal een interdepartementale werkgroep oprichten met als doel om de visie op de impact van digitalisering op de publieke waarden en mensenrechten uit te werken. Die zal ook werken aan onderzoek naar en concrete acties ten aanzien van verdere versteviging van het kader van publieke waarden en mensenrechten.
4. Het ministerie van BZK zal zich richten op dialogen over publieke waarden en mensenrechten en de waarborging hiervan in de informatiesamenleving. Ook zal het proeftuinen mogelijk maken waarin overheden kunnen experimenteren met behoorlijk datagebruik in de openbare ruimte.

120 Zie: https://www.digitaleoverheid.nl/

121 Belangrijke aanjager van de Digitale Agenda en het Digiprogramma van BZK is het rapport *Maak Waar* van de in 2016 ingestelde Studiegroep Informatiesamenleving en Overheid.

Het ministerie van BZK zal verder een aantal onderzoeken (laten) uitvoeren op het gebied van waarborging van publieke waarden en mensenrechten.[122] Zo heeft de Universiteit Utrecht onderzoek gedaan naar de relatie tussen algoritmen en grondrechten (Vetzo et al. 2018). Daarnaast laat BZK onderzoek doen naar de wijze waarop digitalisering deel uit zal maken van het Nationaal actieplan mensenrechten.

Ook doet BZK onderzoek naar het gebruik van (zelf)lerende algoritmen binnen de overheid (Kamerstukken II 2017-2018, 26643, nr 527). In de aangekondigde 'beleidsvisie *open source*' gaat BZK nader in op de mogelijkheden voor het openbaar maken van broncode van geautomatiseerde besluitvorming (Aanhangsel Handelingen II 2017-2018, 1612).[123] Verder wil BZK onderzoek doen naar blockchain en de wet, en naar biometrie.

Op het gebied van digitale democratie heeft BZK de Raad voor het Openbaar Bestuur verzocht om onderzoek te doen naar de kansen en bedreigingen van digitalisering voor een goed functionerende en moderne democratie.

Digitale vaardigheden

Het bevorderen van kennis op het gebied van ICT binnen de overheid is een van de aandachtpunten in de Agenda Digitale Overheid (BZK 2018a). Dit gebeurt voor beslissers via de Algemene Bestuursdienst en verder via het programma Rijksacademie voor Digitalisering en Informatisering Overheid. Ook het vergroten van digitale vaardigheden van burgers vormt een van de aandachtspunten in de Agenda Digitale Overheid. Het kabinet wil samenwerken met maatschappelijke organisaties om het cursusaanbod te vergroten en mensen op weg te helpen. Ook onderzoekt het waar burgers in hun digitale contact met de overheid tegenaan lopen om de eigen systemen te verbeteren. De Tweede Kamer ontvangt voor eind 2018 een aanpak voor digitale inclusie.

Slimme steden

In 2015 hebben steden en de rijksoverheid zich, samen met maatschappelijke partners, gecommitteerd aan het programma *Agenda Stad* om innovatie en leefbaarheid in het Nederlandse stedennetwerk te bevorderen.[124] In 2016 en 2017

122 Overige (aangekondigde) onderzoeken zijn o.a. een adviesaanvraag voor de WRR over de impact van AI op publieke waarden. Het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) laat onderzoek doen naar de juridische aspecten van algoritmen die zelfstandig besluiten nemen.

123 Beantwoording vragen Middendorp en Koopmans over de berichtgeving over het proefschrift van Marlies van Eck van Tilburg University door staatssecretaris Knops.

124 Zie: https://agendastad.nl/

zijn er in dit programma diverse ‘City Deals’ gesloten. Die worden ook genoemd in de kabinetsreactie op de rapporten van het Rathenau Instituut.

Diverse departementen hebben experimenteeromgevingen ingericht om ervaring op te doen met de effecten van technologieën.[125] Ook zijn voor diverse experimenten toetsingskaders opgesteld ter bescherming van het recht op privacy (Kamerstukken II, 2017-2018, 26 643, nr 529). Deze kabinetsperiode komt BZK nog met een Code Goed Digitaal Bestuur om samen met ‘smart cities’ spelregels op te stellen voor het gebruik van gegevens (BZK 2018a).

Desinformatie

Er is binnen BZK ook aandacht voor heimelijke beïnvloeding en desinformatie. Zo schrijft minister Ollongren in een brief aan de Tweede Kamer dat politieke beïnvloeding door statelijke actoren in Nederlandse interne aangelegenheden of democratische processen, zoals de verkiezingen, door de heimelijke inzet van (drog)argumenten, selectieve informatie en desinformatie onwenselijk wordt geacht (Kamerstukken II 2017-2018, 26643, nr 496). In de brief geeft Ollongren aan met media- en technologiebedrijven zoals Facebook, Twitter, Microsoft en Google gesproken te hebben over mogelijke maatregelen. Ook geeft ze aan dat de Nederlandse inlichtingen- en veiligheidsdiensten onderzoek doen naar de intenties en capaciteiten van statelijke actoren, en zijn in het regeerakkoord extra middelen ter beschikking gesteld voor digitale veiligheid. Het kabinet maakt een analyse van mogelijke kwetsbaarheden in het verkiezingsproces.[126]

Privacy en digitale veiligheid

Tot slot werkte het ministerie aan de modernisering van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017). De nieuwe wet introduceert een verruiming van de bevoegdheid van interceptie door de Nederlandse inlichtingen- en veiligheidsdiensten (AIVD en MIVD). Ook zijn nieuwe waarborgen opgesteld, waaronder een toetsing vooraf en een evaluatie van de Wiv na twee jaar. Na het raadgevend referendum op 21 maart 2018, waarin een kleine meerderheid (49,44%) zich tegen de wet uitsprak, heeft het kabinet een aantal aanpassingen gedaan (Kamerstukken 2017-2018, 34588, nr 70). Deze gingen vooral over het delen van informatie met andere landen, de bewaartermijnen en de gerichte inzet van bijzondere bevoegdheden. De Wiv is per 1 mei 2018 in werking getreden.[127]

---

125 Zo is het Living Lab Big Data op het terrein van justitie en veiligheid opgericht om zicht te krijgen op onder andere migratieroutes, migratiemotieven en opleidingsniveaus van asielzoekers en om de datakwaliteit binnen de informatiesystemen te verbeteren. Het traject City Deal ‘Zicht op ondermijning’ is van start gegaan om met behulp van data-analyses patronen met betrekking tot ondermijnende criminaliteit beter te begrijpen.

126 Zie: https://www.tweedekamer.nl/kamerstukken/detail?id=2018Z09600&did=2018D30291

127 Op het gebied van veiligheid is er bovendien aandacht geweest voor de betrouwbaarheid en veiligheid van ondersteunende software bij verkiezingen, het gebruik en de implementatie van vingerafdrukken in paspoorten, en informatiebeveiliging bij de overheid.

Tabel 11 Overzicht maatschappelijke en ethische aspecten digitalisering, ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), op hoofdlijnen (periode 1 januari 2017 - 30 juni 2018)

Wie/wat	Technologie	Issue	Actie
NL DIGIbeter (Agenda Digitale Overheid)	Digitalisering van de overheid	Grondrechten, privacy, veiligheid, autonomie	Benutten van kansen en borgen van rechten voor digitale overheid
Digitale overheid (wetsvoorstel digitale overheid, 'Digitalisering met vertrouwen')	Digitalisering van de overheid	Privacy, veiligheid, vaardigheden, autonomie	Verhogen betrouwbaarheid contact overheid
Kabinetsreactie op 'Opwaarderen' en 'Mensenrechten in het robottijdperk'	Digitalisering	Publieke waarden, mensenrechten (oa privacy, veiligheid, autonomie, controle over technologie)	Kaders en beleidsinstrumenten voor borging publieke waarden
Kabinetsreactie Weten is nog geen doen	Digitalisering	Weerbaarheid, autonomie	O.a. 'doenvermogentoets'
Digitale vaardigheden	Digitalisering	Weerbaarheid, autonomie	Regie op gegevens Aanpak digitale inclusie
Brief heimelijke beïnvloeding door statelijke actoren	Digitalisering, platformen, sociale media	Veiligheid, vrijheid van meningsuiting	O.a. in gesprek met technologiebedrijven onderzoek AIVD & MIVD kwetsbaarheden verkiezingsproces
Slimme steden	Digitalisering	Publieke waarden	Code goed digitaal bestuur
Modernisering Wiv	Digitalisering, communicatie	Digitale veiligheid	Nieuwe bevoegdheden veiligheidsdiensten

Bron: Rathenau Instituut

5.1.2 Ministerie van EZK

Privacy en digitale veiligheid

In het beleid van het ministerie van EZK is sinds lange tijd aandacht voor privacy, digitale veiligheid en vertrouwen. Ook in de periode 2017-2018 staan deze op de beleidsagenda van het ministerie. Het vergroten van weerbaarheid van burgers en organisaties is een van de lijnen van de nationale digitaliseringsagenda: zo is er aandacht voor digitale veiligheidsproblemen met betrekking tot het IoT en voor het MKB is het Digital Trust Center opgericht (zie ook Kamerstukken II, 2017-2018, 26643, nr 488). Verder worden campagnes voor burgers en MKB gekoppeld aan

(nieuw) beleid voor privacy en veiligheid, en zet het kabinet zich in voor de totstandkoming en implementatie van de Europese ePrivacy-verordening.

In de 'Roadmap Digitaal veilige hard- en software' komt het kabinet met maatregelen voor een veiliger IoT (EZK 2018b). Het kabinet zet in op standaarden en certificering van apparaten. Dat blijkt onder meer uit deze acties:

- Nederland dringt in Europese onderhandelingen aan op een snelle vaststelling van de Cyber Security Act, dat een Europees certificeringsraamwerk beoogt voor ICT-producten en –diensten.
- Het kabinet wil op korte termijn verplichte certificering voor bepaalde productiegroepen vaststellen, en deze op langere termijn geleidelijk uitbreiden.
- Ook komt er een monitor met informatie over de digitale veiligheid van IoT-apparaten en een pilot om hard- en software te testen.
- Het kabinet onderzoekt mogelijkheden om aansprakelijkheid rondom onveilige hard- en software te verbeteren. Ook neemt Nederland deel aan de Europese high-level expertgroep over aansprakelijkheid en nieuwe technologieën.
- Nederland stelt in de onderhandelingen over de Europese richtlijn digitale content en diensten voor om fabrikanten te verplichten tot software updates.
- Het kabinet onderzoekt welke minimale veiligheidseisen gesteld kunnen worden aan apparaten via de Europese Radio Equipment Directive, en zal een dialoogsessie voor toezichthoudende instanties organiseren om te bezien welke rol zij kunnen spelen bij de bevordering van digitale veiligheid.
- Het kabinet kijkt welke aanvullende maatregelen er nodig zijn bij het inkoopbeleid van de Rijksoverheid.

Vaardigheden

De toekomst van werk en de veranderende eisen die dat stelt aan de beroepsbevolking is onderdeel van de ambitie 'Iedereen doet mee' uit de nationale digitaliseringsagenda. Naast het moderniseren van het onderwijs met meer aandacht voor digitale vaardigheden (zie paragraaf 5.1.4), wil het kabinet maatschappelijke organisaties en initiatieven ondersteunen om mensen met beperkte digitale vaardigheden extra scholing te bieden. Het ministerie ondersteunt bijvoorbeeld 'Samen Digiwijzer' om de invoering van digitale vaardigheden in het onderwijs te ondersteunen.[128]

Er komt ook een uitwerking van het regeerakkoord op het gebied van een leven lang leren. De Human Capital ICT Agenda heeft als doel het aantal ICT-studenten te vergroten en het Techniekpact probeert het tekort aan ICT-ers terug te dringen. Voor ICT-professionals bij de overheid loopt het programma 'Versterking HR ICT Rijksdienst'.

128 Samen Digiwijzer is een initiatief van CodePact, Mediawijzer.net en Kennisnet en wordt ondersteund door diverse partners. Zie: https://samendigiwijzer.nl/

Platformen en consumentenrechten
Andere onderwerpen op de nationale agenda zijn de kansen en risico's van platformen en consumentenrechten. Het kabinet zet zich op Europees niveau in voor het competitief houden van digitale markten en helderheid over de vraag of aanpassingen aan het mededingingsinstrumentarium nodig zijn. Het kabinet zal zelf onderzoek doen naar verschillende instrumenten, waaronder tarief- en toegangsregulering. De Tweede Kamer zal hierover in het najaar van 2018 worden geïnformeerd (EZk 2018a).

Ook ligt er vanuit de Europese Commissie een voorstel om de zakelijke relatie tussen bedrijven en grote platformen eerlijker en transparanter te maken. Het kabinet onderschrijft het belang van eerlijke en transparante relaties, maar wil voorkomen dat er te veel gedetailleerde eisen aan platformen gesteld worden. Dit zou nadelig kunnen zijn voor kleinere platforms. Het kabinet zet waar mogelijk in op zelfregulering door platforms; mocht dat onvoldoende effectief blijken, dan zal het kabinet kijken of aanvullende regulering nodig is (zoals in het geval van toeristische verhuur van woningen).

Verder liggen er vanuit de Europese Commissie nieuwe wetsvoorstellen voor de bescherming van consumenten. Het kabinet zet daarbij in op versterkte informatieverplichtingen en meer transparantie op platforms over de identiteit van de aanbieder.

Grondrechten en ethiek
Een nieuw onderwerp voor EZK in de periode 2017-2018 is de aandacht voor grondrechten en ethiek in het digitale tijdperk, een van de beleidslijnen in de Nationale Digitaliseringsagenda. De staatssecretaris voor digitalisering heeft aan de WRR een adviesaanvraag gestuurd over AI en publieke waarden (Kamerstukken, 2017-2018, 26 643, nr 529).

Verder kondigt het kabinet aan dat het een nieuw 'nationaal innovatieprogramma over AI zal ontwikkelen, waarin onder meer aandacht zal zijn voor transparantie van algoritmen.

Toekomstbestendige wetgeving
De afgelopen jaren liep het programma toekomstbestendige regelgeving. Het is op 26 juni 2017 afgesloten. Het programma bekeek of wet- en regelgeving als gevolg van technologische ontwikkelingen overbodig zijn, belemmerend zijn of tekortschieten en hoe dat kan worden aangepakt (Kamerstukken II 2016-2017, 33009, nr 42). Op basis van dit programma zijn enkele maatregelen aangekondigd om de transparantie van het wetgevingsproces te vergroten, zoals

internetconsultatie en de digitale wetgevingskalender (Kamerstukken II 2016-2017, 33009, nr 39).

Ook in de komende periode is toekomstbestendige regelgeving een aandachtspunt. Het kabinet geeft aan dat binnen bestaande wet- en regelgeving al veel innovatie mogelijk is. Soms zijn er wel aanpassingen nodig, maar dat kost tijd. Het kabinet geeft in de nationale digitaliseringsagenda aan dat het in een vroeg stadium daarom vaker strategische verkenningen zal laten uitvoeren om de juridische, technologische en ethische consequenties van nieuwe ontwikkelingen te kunnen duiden.

Bedrijvenbeleid
De discussie op het gebied van een *techproof* economie richt zich op een succesvolle digitale transformatie en op het behoud van een sterke concurrentiepositie in het mondiale speelveld. Met het Bedrijvenbeleid 2017 *Navigeren met wind in de zeilen* heeft het kabinet gefocust op duurzame economische groei (EZK 2017).

Naar aanleiding van de motie Ester (Kamerstuk 33 750 XIII, E, 2014), waarin de regering werd verzocht om in het technologie- en innovatiebeleid structureel plaats in te ruimen voor reflectie op ethische vragen, benoemt de monitor enkele activiteiten op dit vlak (Kamerstukken 2015-2016, 33009, nr 16). De monitor verwijst naar onderzoeksprogramma's op Europees en nationaal niveau, zoals Horizon2020 (het SATORI-project waarin een ethische impact assessment is ontwikkeld) en het NWO-programma Maatschappelijk Verantwoord Innoveren, gericht op onderzoek naar maatschappelijke, sociale en ethische aspecten bij innovatie onderzoek. De monitor vermeldt verder dat diverse topsectoren aandacht besteden aan ethische aspecten.

Tabel 12 Overzicht maatschappelijke en ethische aspecten van digitalisering ministerie van Economische Zaken, op hoofdlijnen (periode 1 januari 2017 - 30 juni 2018)

Wie/wat	Technologie	Issue	Actie
Kabinetsreactie op het rapport 'Eerlijk delen' van het Rathenau Instituut	Klusplatforms en deeleconomie	Consumenten-bescherming, openbare orde en privacy	Streven om de negatieve effecten van de deeleconomie te voorkomen of te beperken, en de positieve effecten ervan te stimuleren
Kabinetsreactie op rapport van CPB "Scientia potentia est"	Klusplatforms	Transparantie en aansprakelijkheid	In de Nationale Digitaliseringsstrategie zal aandacht zijn voor de risico's van platforms
Kabinetsreactie op rapport van PBL "Mobiliteit en elektriciteit in het digitale tijdperk"	Digitalisering	Veiligheid	Met de implementatie van de Cybersecuritywet wil EZK de Europese samenwerking bij ICT-incidenten verbeteren
Nationale Digitaliseringsstrategie	Digitalisering	Veiligheid	Specifieke agenda voor de digitalisering van het openbaar bestuur
Roadmap Digitaal veilige hard- en software	Digitalisering, IoT	Veiligheid, aansprakelijkheid	Agenda om veiligheid van verbonden apparaten te vergroten
Digital Trust Center	Digitalisering	Veiligheid, digitale veiligheid	Doel is om bedrijfsleven weerbaarder te maken tegen cyberdreigingen
Platformen en consumentenrechten	Digitalisering, IoT, platformen	Veiligheid, aansprakelijkheid	Problemen van consumenten bij aankopen, onderzoek mededingsinstrumentarium
Human Capital Agenda, Techniekpact	Digitalisering	Digitale vaardigheden	Menselijk kapitaal behouden en vergroten; aansluiting onderwijs op de arbeidsmarkt in de techniekssector
Toekomstbestendige regelgeving	Digitalisering	Wettelijke kaders	Aansluiting wetgeving op technologische ontwikkeling
Bedrijvenbeleid 2017	Technologie	Innovatie	O.a. ethische aspecten in innovatie ontwikkeling

Bron: Rathenau Instituut

5.1.3 Ministerie van JenV

Privacy en digitale veiligheid zijn bekende thema's voor het ministerie van JenV. Nieuw op de agenda zijn de betekenis van algoritmen, profilering en AI, bijvoorbeeld voor de rechtspraak.

Digitale veiligheid
Op 21 april 2018 heeft het ministerie de Nederlandse Cybersecurity Agenda (NCSA) uitgebracht (JenV 2018a). Het is de derde cybersecuritystrategie. De eerste verscheen in 2011, de tweede in 2013. In het regeerakkoord is een structurele investering van 95 miljoen in cybersecurity vastgelegd en deze wordt uitgewerkt in de NCSA. Belangrijke aandachtspunten zijn standaarden voor IoT-apparaten, software-aansprakelijkheid, het stimuleren van cybersecurity-onderzoek en het verbeteren van voorlichtingscampagnes. Beleidsmaatregelen op het vlak van veilige (IoT-)apparaten staan in de Roadmap Digitaal veilige hard- en software (zie EZK 2018b).

Op het vlak van vitale infrastructuur heeft JenV het wetsvoorstel voor de Cybersecuritywet bij de Tweede Kamer ingediend Kamerstukken 2017-2018, 34388, nr G). Het wetsvoorstel vloeit voort uit de Netwerk- en Informatiebeveiligingsrichtlijn (NIB-richtlijn) van de Europese Unie.[129] Met dit voorstel wordt het aantal aanbieders van vitale infrastructuur dat zorg- en meldplichten krijgt, uitgebreid.[130] Met de Cybersecuritywet moeten aanbieders van essentiële diensten, zoals drinkwaterbedrijven, banken en beheerders van gas- en elektriciteitsleidingen, in de loop van 2018 voldoen aan bepaalde beveiligingseisen. Zij moeten adequate maatregelen nemen tegen inbreuken van buitenaf op hun netwerk- en informatiebeveiliging.

Op het gebied van bevoegdheden van opsporingsdiensten is in juni 2018 de Wet Computercriminaliteit III, ook wel de 'terughackwet' genoemd, in de Eerste Kamer aangenomen (Kamerstukken I 2016-2017, 34372). De wet staat politie en justitie toe heimelijk en op afstand (online) onderzoek te doen in computers, servers en mobiele telefoons. De wet wordt twee jaar na inwerkingtreding geëvalueerd.

129 Dit is de eerste cybersecuritywetgeving op Europees niveau en spoort de lidstaten aan hun digitale weerbaarheid te vergroten en beter met elkaar samen te werken.
130 Op dit moment zijn aanbieders onder de Wet gegevensverwerking en meldplicht cybersecurity (Wgmc) 2017 aanbieders van bepaalde diensten alleen verplicht dit soort incidenten te melden bij het Nationaal Cyber Security Centrum (NCSC)

Privacy

In de periode 2017-2018 ging veel aandacht uit naar de invoering van de Algemene verordening gegevensbescherming (AVG). Hiervoor is een Uitvoeringswet Algemene Verordening Gegevensbescherming opgesteld. Beide zijn 25 mei 2018 inwerking getreden.[131] Ook kwam het ministerie met een handleiding voor de nieuwe wet (JenV, 2018b) en een *big data* toolbox, met informatie over het verantwoord toepassen van *big data*.[132]

Verder kwam er een nieuw model voor Privacy Impact Assessments voor nieuwe wetgeving van de Rijksoverheid (Kamerstukken II 2017-2018, 26643, nr 490), en is er een wetsvoorstel verstuurd over implementatie van de Europese PNR-richtlijn (waarbij PNR staat voor 'Passenger Name Records') (2016/681/EU). Die gaat over het gebruik van persoonsgegevens van passagiers voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit (Kamerstukken II 2017/2018, 34861, nr 2).[133]

Het kabinet kondigt aan dat het zijn visie over hoe privacy van burgers onderling (horizontale privacy) kan worden versterkt in het najaar van 2018 naar de Tweede Kamer stuurt.[134]

Tot slot geeft de minister van Rechtsbescherming in het algemeen overleg in de Tweede Kamer over *big data* en de bescherming van persoonsgegevens van 30 mei 2018 aan, dat er een reactie komt op de motie Verhoeven en Van Nispen. Die verzoekt de regering om voor het einde van 2018 de Kamer te informeren over hoe de Autoriteit Persoonsgegevens haar additionele taken en bevoegdheden kan uitvoeren (Kamerstukken II 2017-2018, 34851, nr 23).

Controle over technologie

JenV heeft toenemende aandacht voor algoritmen. Naar aanleiding van de aanbevelingen uit het WRR-rapport *Big data in een vrije en veilige samenleving*

131 Door de AVG worden privacyrechten versterkt en uitgebreid door het recht op vergetelheid en recht op dataportabiliteit. Mensen hebben meer mogelijkheden om voor zichzelf op te komen bij de verwerking van hun gegevens. Zo kunnen mensen eisen dat organisaties persoonsgegevens verwijderen en deze verwijdering doorgeven aan alle andere organisaties die deze gegevens hebben gekregen. Ook hebben mensen recht om van organisaties hun persoonsgegeven in een standaardformaat te ontvangen. Daarnaast krijgen organisaties de verantwoordingsplicht om met documenten te kunnen aantonen dat het de juiste organisatorische en technische maatregelen heeft genomen om aan de AVG te voldoen. Bovendien krijgen Europese privacytoezichthouders meer bevoegdheden, waaronder de bevoegdheid om boetes tot 20 miljoen euro of 4 procent van de wereldwijde omzet op te leggen bij overtreding van de beginselen of grondslagen van de AVG.

132 Zie: https://www.rijksoverheid.nl/documenten/publicaties/2018/04/20/big-data-factsheet. De toolbox bevat o.a. een factsheet *Big data*, 10 uitgangspunten voor experimenteren met *big data*, een modelverwerkinsovereenkomst JenV en een aanvulling op het Model GEB Rijksdienst (PIA) met privacy-aandachtspunten voor *big data*-verwerkingen

133 Luchtvaartmaatschappijen moeten in de loop van 2018 hun passagiersgegevens verstrekken aan de Passagiersinformatie-eenheid Nederland, die tot taak heeft deze informatie te verwerken en te analyseren

134 Hierin zal ook de reactie van het kabinet zijn opgenomen op de initiatiefnota van het Tweede Kamerlid Koopmans over onderlinge privacy (Kamerstukken II 2017-2018, 34926, nr 1-2).

heeft het kabinet tien actiepunten opgesteld (Kamerstukken II, 2016-2017, 26643;32761, nr 426). In mei 2018 geeft de minister voor Rechtsbescherming de stand van zaken met betrekking tot de uitvoering van deze actiepunten weer (Kamerstukken II 2017-2018, 26643/32761, nr 537). De actiepunten gaan onder andere over:

- **een heldere wettelijke basis voor het gebruik van data-analyses**
  Het kabinet beziet of de wettelijke basis voor het uitvoeren en gebruiken van data-analyses versterking behoeft. Hiervoor is een werkgroep gestart, die naar verwachting in de tweede helft van 2018 klaar zal zijn.
- **inzicht in algoritmen**
  Het kabinet onderzoekt hoe voor toezicht en rechterlijke toetsing voldoende inzicht kan worden gegeven in gebruikte algoritmen. Een werkgroep heeft een circulaire (mededeling voor overheidsinstanties) 'Inzicht in algoritmen' opgesteld, die in de *big data* toolbox zal worden opgenomen. De toolbox bevat informatie en richtlijnen voor professionals die werken met *big data*.
  Ook heeft het kabinet onderzocht of het mogelijk is dat bij ICT-overheidsaanbestedingen kan worden vereist dat de meedingende aanbieders algoritmen voldoende inzichtelijk maken voor in elk geval de toezichthouder en de rechter. De uitkomst is dat de Interdepartementale Commissie Bedrijfsjuridisch Advies geen aanleiding ziet om de algemene voorwaarden bij IT-overeenkomsten (ARBIT) aan te passen, omdat 'de behoefte daaraan op dit moment te beperkt is om opneming in de algemene voorwaarden te rechtvaardigen' (Kamerstukken II 2017-2018, 26643/32761, nr 537).
  Verder verzoekt het kabinet de Raad voor de Rechtspraak zich te oriënteren op de kennis die nodig zal zijn om rechtszaken te kunnen behandelen waarbij *big data*-analyses een rol spelen.

Verder zal de minister voor Rechtsbescherming in het najaar van 2018 met een brief komen over de betekenis van algoritmen en AI voor de rechtsspraak (EZK 2018a).

Rechtspositie burgers

Het Wetenschappelijk Onderzoek- en Documentatiecentrum bij JenV (WODC) heeft onderzoek laten uitvoeren of uitbreiding van de mogelijkheden voor burgers en belangenorganisaties, om zich voor een toetsing van *big data*-toepassingen tot de rechter te wenden, mogelijk en wenselijk is. Het onderzoek, uitgevoerd door de Universiteit van Tilburg, is naar verwachting in de tweede helft van 2018 gereed.

Tabel 13 Overzicht activiteiten maatschappelijke en ethische aspecten digitalisering ministerie van Justitie en Veiligheid, op hoofdlijnen (periode 1 januari 2017 - 30 juni 2018)

Wie/wat	Technologie	Issue	Actie
Wet Computercriminaliteit III	Digitalisering	Veiligheid	Nieuwe bevoegdheden veiligheidsdiensten
Algemene verordening gegevensbescherming (AVG), Uitvoeringswet Algemene verordening gegevensbescherming	Digitalisering	Privacy	Privacyrechten worden versterkt en uitgebreid Organisaties krijgen meer verantwoordelijkheden
Toolbox	Digitalisering, *big data* en algoritmen	Privacy	Privacy
Wetsvoorstel PNR-gegevens	Digitalisering	Veiligheid	Registeren van reisgegevens
Visie horizontale privacy	Digitalisering, sociale media, platformen	Privacy	Najaar 2018
Nederlandse Cybersecurity Agenda (NSCA)	Digitalisering, IoT	Veiligheid	Cybersecurity, onderzoek, vaardigheden, vitale infrastructuur
Cybersecuritywet	Digitalisering	Veiligheid	Aanbieders van essentiële diensten moeten voldoen aan beveiligingseisen en adequate maatregelen nemen tegen inbreuken van buitenaf op hun netwerk- en informatiebeveiliging
Kabinetsreactie op rapport van ACVZ “Profileren en selecteren”	Algoritmen	Controle op technologie, rechtvaardigheid (profilering, discriminatie)	JenV kijkt of het huidige juridische kader versterking behoeft
Werkgroep wettelijke basis versterking gebruik data-analyses	*Big data* en algoritmen	Controle op technologie, rechtvaardigheid (profilering, discriminatie)	Tweede helft 2018
Algoritmen in rechtsspraak	*Big data* en algoritmen, AI	Controle op technologie, rechtvaardigheid (profilering, discriminatie)	Tweede helft 2018

WODC-onderzoek juridische aspecten van (zelfstandige) algoritmen	Digitalisering, algoritmen	Controle op technologie, rechtvaardigheid (profilering, discriminatie)	2018
WODC-onderzoek rechtspositie burgers		Autonomie	Mogelijkheden voor burgers en belangenorganisaties om zich voor toetsing *Big data* tot de rechter te wenden, tweede helft 2018

Bron: Rathenau Instituut

5.1.4 Ministerie van OCW

Het ministerie van OCW houdt zich op verschillende manieren bezig met de ethisch-maatschappelijke aspecten van digitalisering. Bestaande thema's zijn onder andere: (digitale) vaardigheden, mediawijsheid, bevordering onafhankelijke journalistiek en mediapluralisme. Nieuw op de agenda zijn het tegengaan van desinformatie en personalisatie van nieuws.

Digitale vaardigheden
Het doel van het kabinet is om in 2021 een nieuw onderwijscurriculum voor het primair en voortgezet onderwijs in werking te laten treden, waarbij er onder andere meer aandacht komt voor digitale geletterdheid (EZK 2018a). Het ministerie van OCW bereidt dit nieuwe curriculum al geruime tijd voor. Zo werd begin 2015 het Platform Onderwijs2032 opgericht. Na oplevering van het eindadvies in 2016, zijn in 2018 negen ontwikkelteams van start gegaan, bestaande uit leraren en schoolleiders uit het primair en voortgezet onderwijs. Begin 2019 worden de opbrengsten met de Tweede Kamer gedeeld voor verdere besluitvorming en om een vervolgproces te bepalen.

OCW voert ook beleid om mediawijsheid onder jongeren te vergroten. Op initiatief van het ministerie is het netwerk *Mediawijzer.net* opgericht: een netwerk van organisaties die samen lespakketten ontwikkelen, publicaties uitgeven en publiekscampagnes opzetten. Dit met als doel dat jongeren, docenten en opvoeders, digitale technologie bewuster en kritischer gebruiken (BZK, 2018a).[135] In de Nationale Digitaliseringsstrategie geeft het kabinet aan dat de aanpak op het gebied van mediawijsheid in de zomer 2018 wordt geëvalueerd en in het najaar de Tweede Kamer hierover zal informeren (EZK 2018a).

135 Zie: https://www.mediawijzer.net/over-mediawijzer-net-2/

Digitalisering in het onderwijs

Het kabinet streeft ernaar om met de inzet van digitale educatieve technologie de kwaliteit van het onderwijs te verhogen (EZK 2018a). De afgelopen jaren is in het Doorbraakproject 'Onderwijs en ICT' gewerkt aan het verbeteren van randvoorwaarden op het gebied van privacy, standaarden en internettoegang. Ook is de inkoopcoöperatie Sivon (Samen Inkopen Voor Onderwijs Nederland) van en voor scholen opgericht. Ook is er een privacyconvenant opgesteld, en er zijn diverse hulpmiddelen gekomen, zoals een *quick scan privacy* en het Sociale Media-protocol (OCW, 2018).

Verder is op 1 februari 2018 de nieuwe Wet pseudonimisering leerlinggegevens in werking getreden (Staatsblad 2018, nr 11). Leerlingen die digitale middelen gebruiken, krijgen een pseudoniem, met als doel privacy van leerlingen beter te beschermen (Kamerstukken II 2016-2017, 34741, nr 2). Er wordt in 2018 gewerkt aan nieuwe beveiligingsstandaarden voor beveiliging. Voor de komende jaren geeft het kabinet in de Nationale Digitaliseringsstrategie aan dat de ministeries van OCW en EZK samen met de PO-Raad, VO-Raad en professionals uit het onderwijs de strategie voor digitalisering in het primair en voortgezet onderwijs zullen verkennen (EZK 2018a).

Desinformatie

Een nieuw onderwerp op de beleidsagenda van OCW is desinformatie en personalisatie van nieuws. Het ministerie organiseerde rondetafels over deze onderwerpen, waarbij ook aandacht was voor onafhankelijke journalistiek. OCW heeft onderzoek laten doen naar desinformatie en de personalisatie van nieuws, en over de toekomst van onafhankelijke journalistiek in Nederland.[136] In juni 2018 zijn deze onderzoeken met de Tweede Kamer gedeeld (Kamerstukken 2017-2018 32827, nr 127). In juni 2018 heeft OCW ook een brief naar de Tweede Kamer gestuurd over de besteding van de in het regeerakkoord vrijgemaakte middelen voor onderzoeksjournalistiek (Kamerstukken II 2017-2018, 32827, nr 126).

136 Naar aanleiding van de motie Heerma/Mohandis (Kamerstukken II 2016-2017, 34550-VIII, nr 82)

Tabel 14 Overzicht activiteiten maatschappelijke en ethische aspecten digitalisering, ministerie OCW, op hoofdlijnen (periode 1 januari 2017 - 30 juni 2018)

Wie/wat	Technologie	Issue	Actie
Aanpassing curriculum primair en voortgezet onderwijs	Digitalisering	Digitale vaardigheden	Digitale geletterdheid in het kerncurriculum van het onderwijs
Mediawijsheid	Digitalisering, sociale media, platformen	Digitale vaardigheden, privacy, veiligheid, online omgangsvormen	Evaluatie aanpak mediawijsheid, najaar 2018
Wet pseudonimisering leerlinggegevens	Digitalisering onderwijs	Privacy	Invoering pseudoniem voor leerlingen die digitale leermiddelen gebruiken
Privacyconvenant, quick scan privacy, sociale media protocol	Digitalisering onderwijs	Privacy, digitale veiligheid	Afspraken en standaarden gegevensverwerking en -beveiliging
Desinformatie en personalisatie van nieuws	Digitalisering, platformen, sociale media	Vrijheid van meningsuiting, bescherming democratie	Rondetafels en onderzoeken. Brief najaar 2018
Toekomst mediabeleid	Digitalisering, platformen, sociale media	Onafhankelijke nieuwsvoorziening, beschermen democratie	Extra middelen onafhankelijke (onderzoeks) journalistiek

Bron: Rathenau Instituut

5.1.5 Ministerie van BuZa

Het ministerie van Buitenlandse Zaken (BuZa) heeft met name aandacht gehad voor digitale veiligheid. Zo heeft BuZa een Internationale Cyberstrategie gepubliceerd, *Digitaal bruggen slaan* (2017).[137] In de Internationale Cyberstrategie wordt aangegeven dat het kabinet zich inzet voor de bevordering en versterking van digitale veiligheid. De inwerkingtreding van de Europese Netwerk- en Informatiebeveiligingsrichtlijn (NIB) is een belangrijke stap waarvan Nederland één van de voortrekkers is. Daarbij zet Nederland in op een aantal speerpunten:

137 Hierin geeft het kabinet invulling aan de toezegging vervat in de kabinetsreactie op de adviezen van de AIV *Het Internet, een wereldwijde vrije ruimte met begrensde staatsmacht* en de WRR *De publieke kern van het Internet: naar een buitenlands internetbeleid*

- Om internationale opsporing in het cyberdomein te bevorderen, zet Nederland in op de intensivering van internationale samenwerking en het versterken van de internationale juridische kaders.
- Om fundamentele rechten en vrijheden internationaal effectief te bestendigen, zet het kabinet in op een mensenrechten en internationaal cyberbeleid. Nederland draagt in internationale fora en 'multistakeholderplatforms' actief bij aan verdere erkenning en waarborging van fundamentele rechten online, om negatieve trends die internetvrijheid in steeds meer landen in de verdrukking brengen te keren.
- Om bescherming en erkenning van het recht op bescherming van persoonsgegevens en het recht op privacy te realiseren, zet het kabinet in op ondersteuning van initiatieven in verschillende multilaterale fora, met als doel om het recht op bescherming van persoonsgegevens en de 'eerbiediging van de persoonlijke levenssfeer' te beschermen en erkennen in de digitale context.

Verder publiceerde het ministerie in mei 2018 *Mensenrechtenrapportage. Actualisering buitenlands mensenrechtenbeleid en resultaten* (BuZa, 2018). Daarin is onder andere aandacht voor internetvrijheid, vrijheid van meningsuiting, vrijheid voor religie en accountability.

Tabel 15 Overzicht activiteiten maatschappelijke en ethische aspecten ministerie van Buitenlandse Zaken, op hoofdlijnen (periode 1 januari 2017 - 30 juni 2018)

Wie/wat	Technologie	Issue	Actie
Internationale Cyberstrategie	Digitalisering	Digitale veiligheid	Inzet voor de bevordering en versterking van digitale veiligheid
Mensenrechten rapportage	Digitalisering	Mensenrechten online	Herbevestiging van Mensenrechtenbrief 2013, Respect en recht voor ieder mens

Bron: Rathenau Instituut

5.2 Eerste en Tweede Kamer

De Eerste en de Tweede Kamer spelen als volksvertegenwoordiging een belangrijke rol bij het genereren van aandacht voor maatschappelijke en ethische vragen over digitalisering. Vanuit hun controlerende taak volgen ze kritisch het regeringsbeleid. In Bijlage 1 staat een overzicht van ingediende Kamervragen en moties op dit gebied voor de periode 1 januari 2017 - 30 juni 2018.

Eerste Kamer
De Eerste Kamer organiseerde diverse deskundigenbijeenkomsten over maatschappelijke en ethische aspecten rondom digitalisering. Zo vroegen de senatoren in 2018 aan deskundigen om toelichting te geven over de staat van de rechtstaat, die onder meer door digitalisering verandert, en in 2017 om toelichting over het vastleggen en bewaren van kentekengegevens door politie en Wet Computercriminaliteit II. Ook vroegen ze om een gesprek met de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD).

De ingediende moties over maatschappelijke en ethische digitaliseringsvraagstukken gaan over deze laatste twee wetsvoorstellen. Ook is er behoefte aan een overkoepelend inzicht in wat digitalisering betekent voor de bescherming van publieke waarden, zie bijvoorbeeld de (aangehouden) motie van het lid Duthler over de vraag ‘of en op welke wijze het proces van digitale transformatie nadere normering behoeft’ (Kamerstukken I 2017-2018, 34 775 VI, V).

Tweede Kamer
In de periode 1 januari 2017 - 30 juni 2018 bouwde de Tweede Kamer actief kennis op over nieuwe maatschappelijke en ethische thema’s via rondetafelgesprekken,[138] onder andere op het gebied van dominantie van technologiebedrijven, de deel- en kluseconomie of AI in het recht. We geven ze hieronder puntsgewijs weer.

Rondetafelgesprekken
De thema’s van de rondetafelgesprekken die het parlement heeft georganiseerd raken met name aan het gebied van de deeleconomie, privacy, en digitale veiligheid. We geven ze hieronder puntsgewijs weer.

- Er was een rondetafelgesprek over *FinTech* in juni 2017, gericht op controle over technologie en hoe technologie de toekomst van de financiële sector zal beïnvloeden. In januari 2018 volgde een rondetafelgesprek over *Cryptocurrencies*.
- In juli 2017 vond een rondetafelgesprek over *Data & Analytics* plaats*,* gericht op de ontwikkelingen op het gebied van data-analyse toegespitst op de Belastingdienst.
- In november 2017 was het rondetafelgesprek *Werk in de platformeconomie,* waarin de kansen en risico’s van online platforms centraal stonden. In januari 2018 volgde naar aanleiding van het rapport *Eerlijk Delen* (2017) van het

138 Bij rondetafelgesprekken nodigen Kamerleden (ervarings)deskundigen uit om toe te lichten hoe zij over het onderwerp denken dat op de agenda staat, waarna ruimte is voor vragen en aanvullingen. Dit soort gesprekken zijn in principe openbaar; er wordt geen verslag van gemaakt

Rathenau Instituut nog een rondetafelgesprek, gericht op het waarborgen van de publieke belangen die een rol spelen bij de deel- en kluseconomie.
- In het rondetafelgesprek *Horizontale privacy* in december 2017 – over hoe burgers onderling omgaan met rechten en plichten rondom privacy – werd besproken of en hoe deze vorm van privacy beter gewaarborgd moet worden.
- In januari 2018 vond een rondetafelgesprek plaats over *Marktdominantie internet- en technologiebedrijven*. Aandachtspunten waren onder meer markttoetreding, mededingingsrecht en de maatschappelijke impact van de marktmacht van enkele grote technologiebedrijven.
- Het rondetafelgesprek *Cybersecurity* in februari 2018 was gericht op de versterking van de weerbaarheid van de Nederlandse samenleving tegen cyberdreigingen.
- In maart 2018 was er een rondetafelgesprek over *Artificiële intelligentie in het recht*, waarbij van belang werd geacht om de grens te bepalen voor welke beslissingen door AI in het recht worden genomen en onder welke voorwaarden.
- In maart 2018 vond ook een rondetafelgesprek over *Drones* plaats. Dat was gericht op een juridisch en regelgevend kader voor het gebruik van drones, onder andere in relatie tot veiligheid, handhaving en privacy.
  In mei 2018 vond er een rondetafelgesprek plaats over internetbedrijven (waaronder Google en Facebook) en privacybescherming.

In de periode van 1 januari 2017 - 30 juni 2018 zijn maatschappelijke effecten van digitalisering ook regelmatig het onderwerp van Kamervragen en moties geweest (zie Bijlage 1). Er is in de Tweede Kamer veel aandacht voor privacy en digitale veiligheid.
- Bij privacy zijn belangrijke onderwerpen het (ongeoorloofd) delen van informatie, gebruik van gegevens voor reclamedoeleinden, de rol van sociale media en de organisatie van het toezicht.
- Bij digitale veiligheid is een belangrijk thema hoe weerbaar Nederland is tegen cyberaanvallen, bijvoorbeeld met het oog op het IoT.
- Relatief nieuwe thema's zijn controle over technologie, rechtvaardigheid en autonomie. De Tweede Kamer wil meer inzicht in algoritmen en mogelijke negatieve effecten ervan (zoals discriminatie). Op het vlak van autonomie werden vragen gesteld over persuasieve technologie (bijvoorbeeld in games, maar ook sociale media), politieke *microtargeting*, de verspreiding van desinformatie, en de vaardigheden en keuzevrijheid van consumenten.

Verder vroeg de Tweede Kamer – rondom het thema menselijke waardigheid en machtsverhoudingen – aandacht voor de macht van platformen, de positie van werknemers en de werkomstandigheden van werknemers. Een nieuw thema dat daarmee te maken heeft, is de mogelijkheid van het belasten van digitale diensten

en platformen. Robotica, biometrie (gezichtsherkenning) en *augmented* en *virtual reality* stonden de afgelopen periode minder prominent op de agenda van de Tweede Kamer.

Ook in de Tweede Kamer bestaat behoefte aan overkoepelend inzicht in wat digitalisering betekent voor de bescherming van publieke waarden, zie bijvoorbeeld de motie van de leden Van Dam en Van der Molen van de Tweede Kamer waarin de regering wordt verzocht om tot een 'waardengedreven benadering van digitalisering te komen' en de Kamer hierover te informeren en de 'gelegenheid te geven bij deze waardenontwikkeling betrokken te raken' (Kamerstukken 2017-2018 32761, nr 120).

Tabel 16 Overzicht activiteiten maatschappelijke en ethische aspecten digitalisering parlement, op hoofdlijnen (periode 1 januari 2017 - 30 juni 2018)

Wie/wat	Technologie	Issue	Actie
Kamervragen en moties	Internet, algoritmen, IoT, platformen, digitalisering breed	Aandacht voor alle 7 publieke waarden (zie tabel 2, hoofdstuk 1)	Vragen om verduidelijking of aanscherping beleid en wet- en regelgeving;
Rondetafelgesprekken	Digitalisering, big data en algoritmen, platformen, AI	Privacy, digitale veiligheid, controle over technologie, rechtvaardigheid, machtsverhoudingen	Kennisopbouw

Bron: Rathenau Instituut

5.3 Europese Commissie

Op Europees niveau geeft de *Agenda Digital Single Market* sinds 2014 de strategische ambities van de Europese Commissie weer.[139] Op basis hiervan bereidt zij hervormingen voor met betrekking tot uiteenlopende juridische kaders, onder andere op het vlak van e-commerce en consumentenbescherming, auteursrecht, audiovisuele en mediadiensten, telecom, privacy en cybersecurity. We gaan hieronder op enkele voorstellen nader in.

139 Zie: https://ec.europa.eu/commission/priorities/digital-single-market/#background

E-Commerce en consumentenbescherming
De Europese Raad heeft in februari 2018 een verordening aangenomen om een einde te maken aan *geoblocking*. Dat verhindert online klanten toegang tot producten of diensten van een website in een andere lidstaat.[140] In april kwam de Europese Commissie met een voorstel voor een 'new deal' voor consumentenbescherming.[141] Een nieuwe richtlijn zal vier bestaande richtlijnen gaan vervangen. Het uitgangspunt van de Commissie is dat de bestaande regelgeving 'doeltreffend' is, en dat er betere mogelijkheden voor handhaving en naleving moeten komen.

Overige wetsvoorstellen hebben betrekking op online aankopen en het bezorgen van diensten, belastingtarieven en dergelijke.

Auteursrecht en illegale content en online platformen
De Europese Commissie heeft nieuwe voorstellen geschreven om het Europees auteursrecht te hervormen.[142] Daarnaast heeft ze op 1 maart 2018 een voorstel aangenomen om illegale content op het internet te bestrijden.[143]

Verder kwam de Commissie op 26 april met een voorstel voor een verordening om eerlijkheid en transparantie bij de interacties tussen bedrijven en online platformen te verbeteren.[144] De verordening bevat een raamwerk met minimale eisen voor transparantie en rechten voor bedrijven om verhaal te halen.

Ook komt er een observatorium voor de online platformeconomie, en een nieuwe richtlijn met regels voor contracten om digitale content aan te bieden.[145]

Desinformatie
In januari 2018 heeft de Europese Commissie de 'High Level Expert Group on Fake News and Online Disinformation' (HLEG) opgericht, die moet gaan adviseren over beleidsinitiatieven om desinformatie en online desinformatie te bestrijden. De expertgroep bracht in maart haar eindrapport uit waarin ze *best practices* voor het tegengaan van desinformatie bespreekt (HLEG, 2018). De expertgroep pleit ervoor om

- de transparantie van online nieuws te verhogen;
- mediawijsheid te stimuleren;

140 Zie: http://europa.eu/rapid/press-release_STATEMENT-18-667_en.htm
141 Zie: http://europa.eu/rapid/press-release_IP-18-3041_en.htm, http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-modernisation-of-consumer-protection-rules
142 Zie: https://ec.europa.eu/digital-single-market/en/modernisation-eu-copyright-rules
143 Zie: https://ec.europa.eu/digital-single-market/en/illegal-content-online-platforms & https://www.eumonitor.nl/9353000/1/j9vvik7m1c3gyxp/vki0gceun8zi
144 Zie: https://ec.europa.eu/digital-single-market/en/news/regulation-promoting-fairness-and-transparency-business-users-online-intermediation-services
145 Zie: http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2018)614707

- tools te ontwikkelen om gebruikers en journalisten te helpen om desinformatie tegen te gaan;
- de diversiteit van het media-ecosysteem te bewaken; en
- de impact van desinformatie te monitoren en beleidsmaatregelen te evalueren (EC, 2018a).

Op 26 april kwam de Europese Commissie met een zogenoemde communicatie voor een Europese aanpak voor het tegengaan van desinformatie.[146] Ze stelt onder meer voor dat online platformen een *code of practice* ontwikkelen, waarin oog is voor:

- transparantie van gesponsorde content;
- de werking van algoritmen; en
- maatregelen om nepaccounts en automatische bots tegen te gaan.

Ook wil de Commissie dat:

- er een Europees onafhankelijk netwerk komt van factcheckers;
- mediawijsheid wordt vergroot;
- lidstaten worden ondersteund om verkiezingen weerbaar te maken tegen cyberdreigingen;
- vrijwillige online identificatiesystemen worden gestimuleerd.

Tot slot wil de Europese Commissie dat de lidstaten meer doen om kwaliteit van journalistiek en diversiteit van informatie te waarborgen.

Privacy en digitale veiligheid

In mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. Op het gebied van privacy werkte de Europese Commissie in de afgelopen periode ook aan de herziening van de ePrivacy-verordening.[147] Het voorstel hiervoor bevat specifieke privacyregelgeving voor de elektronische communicatiesector, die onder meer moeten gelden voor platformen zoals Whatsapp, Facebook Messenger en Skype. Het voorstel heeft ook als doel de cookiebepalingen te versimpelen.

De Europese Commissie heeft daarnaast in 2017 een wetsvoorstel ingediend voor de ‘Cybersecurity Act’ (2017/0225/COD), waarmee het Europese Cybersecurity Certificeringskader voor ICT-producten en diensten kan worden vastgesteld. Het specificeert ook de taken en functies van het Europese Agentschap voor Netwerk- en Informatiebeveiliging (ENISA) op het gebied van cyberveiligheid-certificering.

146 Zie: http://europa.eu/rapid/press-release_IP-18-3370_en.htm & https://ec.europa.eu/digital-single-market/en/news/communication-tackling-online-disinformation-european-approach
147 Zie: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

Audiovisuele mediadiensten
Op 26 april 2018 bereikten het Europees Parlement, de Europese Raad en de Europese Commissie voorlopige overeenstemming over de herziening van de richtlijn over audiovisuele mediadiensten.[148] De nieuwe richtlijn breidt onder meer de regels uit voor het beschermen van jongeren; ook is er op het vlak van haat zaaien een uitbreiding van mediadiensten naar videodiensten. Verder versterkt de richtlijn de onafhankelijkheid van de toezichthouders op dit vlak.

Drie prioriteiten
In de *mid-term review* (mei 2017) van de Digitale Agenda identificeerde de Commissie drie kerngebieden waarop verdere actie nodig is: online platformen, data-economie en cybersecurity.[149] In maart 2018 kwam de Europese Commissie met nieuwe voorstellen om digitale bedrijven, zoals Facebook en Apple, belasting te laten betalen in de Europese Unie. Dit voorstel wordt dit jaar besproken met de Europese Commissie en de lidstaten.[150] Ook verkent de Europese Commissie een aantal nieuwe beleidsprioriteiten, waaronder digitale vaardigheden en AI.[151]

In mei 2018 lanceerde de Europese Commissie een communicatie over AI (EC, 2018c), die voortvloeit uit de de kort daarvoor afgelegde verklaring van 25 Europese lidstaten om samen te werken op het gebied van AI.[152] De communicatie richt zich op drie speerpunten:
1. het verhogen van de publiek-private investeringen in de ontwikkeling van AI;
2. het voorbereiden op socio-economische veranderingen (zoals modernisering van het onderwijs); en
3. het zorgdragen voor een geschikt ethisch en juridisch raamwerk.

De Commissie zal samen met de lidstaten een gecoördineerd AI-plan opstellen. Dat wordt eind 2018 verwacht.[153] Ook het concept van de ethische richtlijnen zal eind 2018 worden gepubliceerd. De Europese strategie zal in samenwerking met de High Level Expert Group on Artificial Intelligence worden uitgewerkt.[154] De Commissie heeft ook de European AI Alliance gelanceerd, een forum voor discussie waar stakeholders input kunnen leveren voor deze High Level Expert

148 Zie: http://europa.eu/rapid/press-release_IP-18-3567_en.htm
149 Zie: https://ec.europa.eu/digital-single-market/en/news/digital-single-market-mid-term-review & https://ec.europa.eu/commission/commissioners/2014-2019/ansip/announcements/statement-vice-president-ansip-press-conference-mid-term-review-digital-single-market-strategy_en
150 Zie: http://europa.eu/rapid/press-release_IP-18-2041_en.htm
151 Overige gebieden zijn digitale industrie, 'high performance computing', het moderniseren van publieke en egovernmentdiensten en gezondheidszorg, Zie: https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market
152 Zie: https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence
153 Zie: http://europa.eu/rapid/press-release_IP-18-3362_nl.htm
154 Zie: https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

Group.[155] Bij de AI-strategie hoort ook dat de Europese Commissie naar juridische kaders kijkt op het gebied van veiligheid, verantwoordelijkheid en aansprakelijkheid. Ook voor dit onderwerp heeft ze een expertgroep ingesteld.[156] Deze groep zal haar assisteren bij de vraag of de huidige regelgeving in de Europese Unie geschikt is voor nieuwe technologieën als AI, robotica en het IoT.

155 Zie: https://ec.europa.eu/digital-single-market/en/european-ai-alliance
156 Zie: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=615947

Tabel 17 Overzicht activiteiten Europese Commissie maatschappelijke en ethische aspecten digitalisering, op hoofdlijnen (periode 1 januari 2017 - 30 juni 2018)

Wie/wat	Technologie	Issue	Actie
E-commerce en consumentenbescher ming	Digitalisering, sociale media, platformen	Privacy, autonomie, rechtvaardigheid, machtsverhoudingen	O.a. modernisering consumentenrecht, en geoblocking
Auteursrecht, illegale content en platformen	Digitaliseirng, sociale media, platformen	Privacy, autonomie, rechtvaardigheid, machtsverhoudingen	Voorstellen auteursrecht, illegale content, relatie platformen-bedrijven, digitale content
Desinformatie	Digitalisering, sociale media, platformen, persuasieve technologie	Autonomie (manipulatie, vrijheid van meningsuiting), bescherming democratie	Expertgroep over fake nieuws en desinformatie; advisering beleidsinitiatieven Communicatie met beleidsvoornemens tegengaan desinformatie
Privacy en digitale veiligheid	Digitalisering, IoT sociale media, platformen	Privacy, veiligheid	AVG 25 mei 2018 in werking getreden ePrivacy – onderhandelingen Cyber Security Act
Audiovisuele mediadiensten	Digitalisering, sociale media, platformen	Veiligheid, autonomie, onafhankelijke nieuwsvoorziening, pluralisme media-aanbod	Herziening richtlijn, oa. uitbreiding regels naar videodiensten, versterking onafhankelijkheid toezichthouders
Digitale belasting voorstel	Digitalisering, platformen	Rechtvaardigheid, machtsverhoudingen	Voorstel om in meer lidstaten belasting te heffen van digitale bedrijven
AI	AI	Innovatie, vaardigheden, arbeidsmarkt, ethische en juridische aspecten	AI-strategie, expertgroep AI. Stimuleren van innovatie, vaardigheden en ethische aspecten

Bron: Rathenau Instituut

5.4 Europees Parlement

Ook op het niveau van het Europees Parlement waren er in de periode 2017-2018 veel ontwikkelingen op de genoemde thema's. We noemen hier enkele opvallende ontwikkelingen, waarbij we met name kijken naar aangenomen resoluties.

Het Europees Parlement (EP) heeft de resolutie *Civil Law Rules on Robotics* (2015/2103/INL) aangenomen, met aanbevelingen aan de Europese Commissie over civiele rechten met betrekking tot robotica. De leden vonden het essentieel dat er een garantie is dat mensen altijd de controle hebben over intelligente machines, wanneer ze met robotica en AI werken. Ook benadrukte het parlement dat een duidelijk, strikt en efficiënt leidend ethisch raamwerk nodig is voor het ontwikkelen, ontwerpen, produceren, gebruiken en aanpassen van robots.

Het EP besteedt in zijn resoluties veel aandacht aan de relatie tussen platformen, machtsverhoudingen en mensenrechten. Volgens het EP bieden digitale platforms en diensten nieuwe kansen op de markt, maar ook maatschappelijke uitdagingen:

- In de resolutie *Naar een digitale handelsstrategie* (2017/2065(INI)) doet het dat met betrekking tot digitale handel en het waarborgen van consumentenrechten en mensenrechten.
- De resolutie *De digitalisering van de Europese industrie* (2016/2271(INI)) uit juni 2017, roept op tot een strategie die 'de meest urgente economische en maatschappelijke uitdagingen voor Europa' van digitalisering aanpakt.[157] Hier heeft het EP o.a. aandacht voor de maatschappelijke gevolgen van de deeleconomie. Daarvoor zijn ook in juni aparte resoluties aangenomen:
  a. de *Europese agenda voor de deeleconomie* (2017/2003(INI));
  b. en *Onlineplatforms en de digitale eengemaakte markt* (2016/2276(INI))
  Deze resoluties vragen om een eerlijke concurrentiepositie voor bedrijven, consumenten en instanties ten opzichte van de deeleconomie.

Een andere belangrijke publieke waarde voor het EP was rechtvaardigheid en dan met name de positie van vrouwen. Zo stipte het in twee resoluties respectievelijk de positie en kansen van vrouwen online en van vrouwen in digitale sectoren aan (EP, 2017/2210(INI); 2017/3016(RSP)).

Ten slotte nam het EP resoluties aan over privacy en gegevensbescherming:

- *De strijd tegen cybercriminaliteit* (2017/2068(INI)), oktober 2017;
- *De gevolgen van big data voor de grondrechten* (2016/2225(INI)), maart 2017;
- *Een Europese strategie voor coöperatieve slimme vervoerssystemen* (2017/2067(INI)), maart 2017;
- *Resolutie van het Europees Parlement over de gepastheid van de door het EU-VS-privacyschild geboden bescherming* (2018/2645(RSP)), juni 2018.

Buitenlandse voorbeelden

Ook in het buitenland gebeurt veel op het vlak van maatschappelijke en ethische digitalisering. We noemen hier enkele opvallende voorbeelden.

157 Zie: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0183+0+DOC+XML+V0//NL

- **Japan** heeft een wettelijk voorgeschreven vijfjaarlijkse wetenschaps- en technologiestrategie geïntroduceerd (5th Science and Technology Basic Plan, 2016-2020). Hierin introduceert het onder de noemer 'Society 5.0' een visie voor een duurzame, welvarende en inclusieve toekomst met behulp van technologie. Japan hoopt hiermee oplossingen voor maatschappelijke problemen te kunnen bieden, zoals het lage geboortecijfer en de vergrijzende bevolking. Hiervoor moeten op vijf gebieden 'doorbraken' worden gerealiseerd, onder andere bij de manier waarop de overheid werkt, op juridisch gebied, op technologiegebied, op de beschikbaarheid van menselijk kapitaal en op het gebied van maatschappelijke acceptatie van technologie.

- In het **Verenigd Koninkrijk** heeft een commissie van het Britse parlement een *AI Code* gepubliceerd voor ontwikkelaars en gebruikers van intelligente systemen in het rapport. De code is gericht op de ethische implicaties van AI (Authority of the House of Lords, 2018). Om het Verenigd Koninkrijk veilig en ethisch gebruik te laten maken van AI, en hier wereldwijd een sterke positie in te blijven houden, stelt de commissie vijf principes voor: 1) AI moet ten goede komen aan de gemeenschap, 2) AI moet gebaseerd zijn op eerlijkheid en uitlegbaarheid, 3) AI moet niet worden gebruikt om privacy of datarechten van individuen, families of gemeenschappen te verminderen, 4) alle burgers hebben het recht om onderwezen te worden zodat ze mentaal en emotioneel goed kunnen gedijen, en 5) de autonome macht om mensen pijn te doen, vernietigen of te misleiden, mag AI nooit toekomen. Inmiddels heeft het land een *AI Sector Deal* om investeringen in AI aangekondigd.[158]

- **Frankrijk** introduceerde op 29 maart 2018 een AI-strategie 'AI for humanity', met als doel Frankrijk de Europese leider te maken op het gebied van AI, en een AI-ecosysteem te bouwen in Europa (Villani, 2018). De strategie bestaat uit zes pijlers: het opbouwen van een op data gericht economisch beleid, investeren in Frans AI-onderzoek, het inzetten van AI voor duurzaamheid, ethische aspecten van AI, en inclusieve AI. Voor het waarborgen van ethische aspecten beveelt het rapport het oprichten van een ethische commissie aan. Als onderdeel van de AI-strategie wil president Macron 1,5 miljard euro investeren in Frans AI-onderzoek.

- Sinds 1 januari is in **Duitsland** de 'Netzwerkdurchsetzungsgesetz' (de netwerkhandhavingswet) van kracht. Die verplicht sociale media maatregelen te nemen tegen het strafbare haatzaaien op hun platformen. De platformen zijn verplicht haatzaaiende content te verwijderen, anders kunnen ze een boete krijgen (Artikel 1 G. v. 01.09.2017 BGBl. I S. 3352, Nr. 61). Daarnaast heeft de

[158] Zie: https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal

ethische commissie voor het Duitse ministerie voor Transport en Digitale Infrastructuur ethische richtlijnen geformuleerd voor zelfrijdende auto's (BMVI 2017). De richtlijnen gaan onder andere over situaties waarin schade onvermijdbaar is, de beschikbaarheid en beveiliging van data, de interactie tussen mens en de zelfrijdende auto, en bredere implicaties van zelfrijdende auto's. Veiligheid is een belangrijk uitgangspunt van de richtlijnen, evenals non-discriminatie. Volgens de richtlijnen is het de auto's niet toegestaan bij een onvermijdbaar ongeluk te discrimineren op basis van persoonlijke eigenschappen (ras, geslacht, of mentale toestand).

Tabel 18 Voorbeelden buitenland maatschappelijke en ethische aspecten digitalisering, periode 1 januari 2017 - 30 juni 2018

Wie/wat	Technologie	Issue	Actie
Verenigd Koninkrijk – AI code	AI	Privacy, veiligheid, controle over technologie, rechtvaardigheid, menselijke waardigheid, inclusie	5 uitgangspunten voor AI code om ontwikkelingen te sturen en risico's van AI te verzachten
Frankrijk – AI-strategie	AI	Controle over technologie, menselijke waardighied, machtsverhoudingen, inclusie	AI-strategie: o.a. op data gericht economisch beleid, effecten arbeidsmarkt en ethische aspecten AI (opzet ethische commissie)
Duitsland – netwerkhandhavings-wet	Sociale media	Veiligheid	Wet verplicht sociale media maatregelen te nemen tegen strafbaar haatzaaien op hun platformen
Duitsland – Ministerie voor Transport en Digitale Infrastructuur	Zelfrijdende auto's	Veiligheid, controle over technologie, rechtvaardigheid	Ethische richtlijnen door de ethische commissie voor zelfrijdende auto's
Japan – Society 5.0	IoT, big data, AI, robotica, platformen	Kwaliteit van leven, duurzaamheid, ethische aspecten	Vijfjaarlijkse wetenschaps- en technologiestrategie, oa. ethische aspecten technologie

Bron: Rathenau Instituut

5.5 Conclusie

Ethiek en grondrechten op de nationale beleidsagenda
In *Opwaarderen* zagen we dat met name kwesties als privacy en digitale veiligheid op de beleidsagenda's van diverse ministeries stonden. Er was ook weinig aandacht voor een overkoepelende visie op de betekenis van digitalisering. In de periode 1 januari 2017 - 30 juni 2018 is daar verandering in gekomen. Er staat nu een breed palet aan maatschappelijke en ethische kwesties op de agenda.

Met het aantreden van het nieuwe kabinet zijn er in de eerste helft van 2018 diverse nationale agenda's aangekondigd, waaronder in juni de overkoepelende Nationale Digitaliseringsagenda (ook in de tweede helft van 2018 zullen nog diverse nota's verschijnen, onder meer over open source, horizontale privacy, mediawijsheid en AI in de rechtspraak). In de gepubliceerde agenda's vormen ethiek en grondrechten onderdeel van de beleidslijnen. Maatschappelijke en ethische kwesties zijn daarmee duidelijk op de nationale agenda gekomen. In de agenda's benadrukt het kabinet dat de samenleving voor een transitie staat, met positieve en negatieve kanten, en dat digitalisering niet meer slechts een zaak is voor de uitvoering, maar een 'Chefsache': een onderwerp voor de bestuurstafel (BZK 2018b, 2).

Privacy en digitale veiligheid
Ook vanaf 2017 is er op nationaal niveau veel aandacht voor privacy en digitale veiligheid. Op het gebied van privacy bestaat al lang wetgeving. Per 25 mei 2018 is de Europese Algemene verordening persoonsgegevens (AVG) in werking getreden. Op het gebied van digitale veiligheid zijn veel nieuwe beleidsmaatregelen aangekondigd. Op dit terrein is de stap gemaakt van agendavorming naar beleidsbepaling. Zo is in Nederland onder andere de Cybersecuritywet aangenomen, is er voor het midden- en kleinbedrijf een Digital Trust Centrum opgericht om meer kennis en informatie te kunnen uitwisselen (zo'n centrum was er tot nu toe vooral voor 'vitale' sectoren) en is er een roadmap opgesteld voor veilige hard- en software, met concrete maatregelen om IoT-apparaten beter te beveiligen.

Verkenning van nieuwe thema's
Er zijn ook nieuwe onderwerpen op de beleidsagenda gekomen, zoals de verspreiding van desinformatie, invloed van digitalisering op democratie, de invloed van algoritmen, grondrechten, digitale vaardigheden en machtsverhoudingen. Hier bevindt de beleidsvorming zich nog in een verkennende fase. Het kabinet heeft op een breed gebied nieuwe onderzoeken aangekondigd, of het onderzoek is in uitvoering. Voorbeelden zijn onderzoek naar het gebruik van algoritmen binnen de overheid, onderzoek naar digitalisering van de democratie en onderzoek naar de betekenis van AI en de bescherming van publieke waarden.

Wettelijke kaders
Het kabinet kijkt op diverse plekken in hoeverre huidige wettelijke kaders voldoen, en of aanpassingen nodig zijn. Zo laat het kabinet onderzoeken in hoeverre het huidige mededingingsinstrumentarium nog voldoet. Ook wil het de relatie tussen blockchain en de wet onderzoeken, en bekijkt het bijvoorbeeld of versterking nodig is voor het wettelijk kader voor het uitvoeren en gebruiken van data-analyses (Kamerstukken II 2016-2017, 266423/32761, nr 426).

Eerste en Tweede Kamer
Het Nederlandse parlement heeft veel aandacht voor privacy en digitale veiligheid. Daarnaast zijn ook nieuwe thema's op de agenda van de Eerste en Tweede Kamer gekomen, zoals controle over technologie (inzicht in algoritmen), rechtvaardigheid (discriminatie door algoritmen), autonomie (over desinformatie, politieke *microtargeting* en keuzevrijheid), en menselijke waardigheid en machtsverhoudingen (positie van deel- en klusplatformen, omstandigheden werknemers en macht van technologiebedrijven).

Via rondetafelgesprekken en deskundigenbijeenkomsten bouwen de Eerste en Tweede Kamer actief kennis op rondom nieuwe maatschappelijke en ethische digitaliseringskwesties, bijvoorbeeld op het vlak van digitalisering en de rechtspraak, data-analytics of de deel- en kluseconomie.

Internationaal niveau
Ook bij de Europese Commissie staan digitalisering, en de maatschappelijke en ethische aspecten daarvan, nadrukkelijk op de agenda. Op basis van de Agenda Digital Single Market bereidt de Commissie hervorming voor met betrekking tot tal van juridische kaders, onder meer op het vlak van relaties tussen bedrijven en platformen, en op het gebied van consumentenrechten, geoblocking, auteursrecht, audiovisuele en mediadiensten, illegale content, privacy en digitale veiligheid. Nieuwe onderwerpen voor de Commissie zijn verspreiding van desinformatie, aansprakelijkheidkwesties rondom nieuwe technologieën, en AI. Verder vormen de data-economie en cybersecurity belangrijke prioriteiten van de Europese Commissie.

6 Politiek en bestuur: toezichthouders

In de fase van beleidsuitvoering gaat het er om dat toezichthouders en toetsingscommissies ervoor zorgen dat de regels, normen en wetten worden geïmplementeerd en nageleefd. Een toezichthouder is een door de overheid aangesteld, onafhankelijk en onpartijdig instituut dat toeziet op naleving van wet- en regelgeving door organisaties. We richten ons in dit hoofdstuk op nationale toezichthouders die relevant zijn voor maatschappelijke en ethische aspecten van digitalisering en overige organisaties, zoals de Nationale ombudsman en het Nationaal Cyber Security Centrum.

We zien dat bij veel toezichthouders het bewustzijn voor maatschappelijke en ethische aspecten van digitalisering toeneemt, bijvoorbeeld op het gebied van media en reclame, de financiële markten of marktmacht van platformen. Diverse toezichthouders oriënteren zich op de betekenis van digitalisering voor hun domein of bouwen nieuwe kennis op. In de periode 2017-2018 is bij diverse toezichthouders het mandaat vergroot of aangepast, en is er sprake van een verhoogd budget of capaciteit.

6.1 Nederland

Autoriteit Persoonsgegevens
De Autoriteit Persoonsgegevens (AP) ziet toe op de naleving van de privacywetgeving en adviseert over nieuwe wet- en regelgeving. Een belangrijk thema voor de AP in 2017 was de nieuwe EU-privacywetgeving in de vorm van de AVG, die per 25 mei 2018 in werking is getreden. De AP gaf veel voorlichting over de aankomende wetgeving[159] en reorganiseerde de eigen organisatie, met het oog op de uitbreiding van taken en bevoegdheden (AP 2018). De AP is vanaf 25 mei 2018 bijvoorbeeld verplicht om elke klacht van burgers in behandeling te nemen. Eind juni 2018 berichtte de AP dat sinds de inwerkingtreding van de nieuwe wet 600 mensen privacyklachten hadden ingediend.[160] Verder is met de nieuwe wet ook de boetebevoegdheid verhoogd en groeit het aantal medewerkers bij de

159 Zie bijvoorbeeld: https://autoriteitpersoonsgegevens.nl/nl/nieuws/start-campagne-privacy-gaat-iedereen-wat-aan
160 Zie: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ruim-600-mensen-dienen-privacyklacht-bij-ap

toezichthouder. Het kabinet zal het budget van de AP in 2018 verhogen met 5 miljoen euro en in 2019 met 2 miljoen euro (Kamerstukken II, 2017-2018, 26643, nr 529).[161]

Naast de AVG waren andere thema's voor de AP in 2017 transparantie bij profilering, verwerking van bijzondere persoonsgegevens, en beveiliging van persoonsgegevens (AP, 2017a). Wat dat laatste betreft drong de AP bij Airbnb aan op het staken van het verwerken van Burgerservicenummers (BSN). Inmiddels verwijdert Airbnb automatisch het BSN uit alle digitale kopieën van identiteitsbewijzen en heeft het alle BSN's van eerder verzamelde identiteitsbewijzen vernietigd.[162] Verder gaf de AP in 2017 onder andere adviezen over wetsvoorstellen zoals de Wet Basisregistratie Personen (BRP) (AP, 2017b), Wet Passagiers Namen Register (PNR) (AP, 2017c), Implementatiewet Payment Service Directive 2 (PSD2) (AP, 2017d), en Cybersecuritywet (AP, 2017e).

Ook het gebruik van persoonsgegevens door sociale media heeft de aandacht van de AP. In 2017 deed zij met een aantal toezichthouders in Europa onderzoek naar de verwerking van persoonsgegevens door Facebook. Uit het onderzoek bleek dat Facebook gebruikers onvolledig informeerde over het gebruik van hun persoonsgegevens. Ook stelde de AP vast dat Facebook bijzondere gegevens van gevoelige aard gebruikt zonder uitdrukkelijke toestemming van de gebruikers. Zo verwerkte het platform de gegevens over seksuele geaardheid om op basis hiervan gerichte advertenties te tonen. Facebook is met dit laatste inmiddels gestopt (AP, 2017). Naar aanleiding van de berichtgeving over Cambridge Analytica, kondigde een werkgroep van Europese toezichthouders, waaronder de AP, in 2018 aan om te kijken naar hoe socialemediaplatformen aan hun gegevens komen en hoe de platformen voorkomen dat anderen daar onrechtmatig toegang toe hebben.[163]

Autoriteit Consument en Markt

De Autoriteit Consument en Markt (ACM) houdt toezicht op mededinging, telecommunicatie en consumentenrecht. In 2016-2017 was een van de speerpunten van de ACM 'Digitalisering – de online consument'. Het speerpunt was gericht op het voorkomen van concurrentie- en consumentenproblemen op internet, en monitoren of bedrijven dankzij het gebruik van persoonsgegevens hun machtspositie op internet vergroten. In 2018-2019 vormt de digitale economie een belangrijk onderdeel van de agenda.[164] Het ACM wil zich in het bijzonder richten op

161 In 2017 onderzocht adviesbureau Andersson Elffers Felix hoeveel capaciteit en middelen de AP in de toekomst nodig heeft. Het kwam tot drie scenario's voor het verwachte extra budget (bovenop het huidige budget van 7,7 miljoen): laag 12 miljoen, midden 16 miljoen, hoog 22 miljoen (Kamerstukken 2016-2017, 32761, nr 112).

162 Zie: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-airbnb-be%C3%ABindigt-verwerking-bsn

163 Zie: https://autoriteitpersoonsgegevens.nl/nl/nieuws/europese-privacytoezichthouders-trekken-samen-op-aanpak-social-media

164 Zie: https://denkmee.acm.nl/thema/digitale-economie?status=inactief

een goede en open infrastructuur voor een snel en betaalbaar internet, de macht van bedrijven door gebruik van data en algoritmes, en duidelijke informatie en keuzevrijheid voor online consumenten (zie ook *Het Signaal 2018* van ACM).

ACM richt zich in haar strategie op drie pijlers, namelijk:
1. investeren in kennis over de werking van digitale markten;
2. actief volgen van ontwikkelingen; en
3. inzetten op internationale en nationale samenwerking (ACM, 2018).

Ook zal ACM een speciaal team oprichten op het gebied van digitale mededinging (Regeerakkoord 2017-2021; EZK 2018a). Verder nam ACM samen met andere Europese toezichthouders de algemene voorwaarden van socialemediaplatformen onder de loep, bijvoorbeeld rond het recht om een koop te ontbinden en de gang naar een lokale rechter in plaats van een Amerikaanse rechter. Diverse platformen hebben al naar tevredenheid van de toezichthouders de voorwaarden aangepast, anderen hebben toegezegd deze door te voeren.[165] Samen met het Commissariaat voor de Media (CvdM) deed ACM in 2018 ook onderzoek naar de digitalisering van het nieuws (zie hieronder).

College voor de Rechten van de Mens

Het College voor de Rechten van de Mens (CRvdM) 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.[166] In zijn strategisch plan 2016-2019 refereert het College niet aan de manier waarop technologische ontwikkelingen aan mensenrechten raken. Er is dan ook geen apart rapport gericht op digitalisering en mensenrechten.

Waar relevant besteedt het College wel aandacht aan gevolgen van digitalisering voor mensenrechten, zoals bij toegang tot informatie. Als toezichthouder op het VN-verdrag inzake de rechten van personen met een handicap stelt het College mensen met een beperking die niet meekunnen in de samenleving centraal. Het College heeft onder andere als taak om bewustwording hierover te vergroten. Zo richt het College zich onder andere op het recht op toegang tot informatie, zoals in het geval van de digitale toegankelijkheid van websites voor mensen met een handicap, op grond van de Algemene wet gelijke behandeling en het VN-verdrag, of voor ouderen.[167] Zo stelt het College in zijn rapportage over de toegankelijkheid van verkiezingen voor mensen met een beperking (CRvdM, 2017a) dat digitaal stemmen in het stemlokaal als oplossing werd beschouwd. Daarnaast stelt het

165 Zie: https://www.acm.nl/nl/publicaties/social-mediaplatforms-google-facebook-en-twitter-passen-algemene-voorwaarden-aan-onder-druk-europese-toezichthouders
166 Wet College voor de Rechten van de Mens (Staatsblad 2011, 573)
167 Er is bijvoorbeeld een rapport over de gemeentelijke websites: https://mensenrechten.nl/publicaties/detail/35682

College in zijn advies (CRvdM, 2017b), naar aanleiding van het wetsvoorstel 'Generieke digitale infrastructuur', dat toegang tot digitale informatie voor mensen met een beperking van groot belang is en dat toegankelijkheid (wat ook geldt voor digitale toegankelijkheid) een van de grondbeginselen van het VN-verdrag is.

Ook vindt er afstemming plaats tussen het College en andere toezichthouders zoals de AP en de Nationale ombudsman, die ook in de Raad van Advies van het College zitten. Ten slotte is er in de afgelopen periode van 2016-2018 geen specifieke uitbreiding van het budget van het College geweest voor digitalisering, maar wel voor nieuwe taken met betrekking tot het VN-verdrag.

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 Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Ze onderzoekt de rechtmatigheid van operaties en dataverzameling door veiligheidsdiensten, en wordt ingeschakeld als onafhankelijke adviescommissie bij klachten over het handelen van de veiligheidsdiensten (CTIVD, 2017). Belangrijke onderwerpen voor de CTIVD zijn onder meer de balans tussen nationale veiligheid en rechtsbescherming van de burger, transparantie, en het maatschappelijk debat. In haar onafhankelijke rol zal de CTIVD haar toezicht mede op basis van deze onderwerpen vormgeven. Hierdoor zullen onderwerpen als 'kabelgebonden bulkinterceptie',[168] geautomatiseerde data-analyse en datareductie belangrijke thema's zijn.[169]

Als gevolg van de invoering van de Wet op de Inlichtingen- en Veiligheidsdiensten 2017 (Wiv, 2017) is het mandaat van de CTIVD veranderd. Zo zal met de invoering van de Wiv 2017 de CTIVD bestaan uit een afdeling toezicht en een afdeling klachtbehandeling, waarbij het klachtrecht bindend zal zijn. De toezichtstaak blijft ongewijzigd en betreft niet-bindend toezicht achteraf. Ook is het budget van de CTIVD al in 2016 uitgebreid, en met de invoering van de Wiv 2017 verder uitgebreid in 2018. Deze uitbreiding voorziet onder andere in de personele uitbreiding van de CTIVD, zoals de uitbreiding als gevolg van de afdeling klachtbehandeling en de formatie van een ICT-unit.

Ook zal de CTIVD met de ingang van de Wiv 2017 intensief toezicht uitoefenen op de activiteiten van de AIVD en MIVD, met name waar het gaat om de (gerichtheid van de) nieuwe bevoegdheden, zoals het in bulk aftappen van de kabel, het proces

168 Dit is het verzamelen en filteren van gegevens die zijn verzameld via het internet (de kabel); voorheen mochten de diensten dit alleen door voor internetverkeer via de ether.
169 Gesprek met Frank Brasz van CTIVD op 4 april 2018.

van verantwoorde databeperking tijdens de verwerking van gegevens, en de toepassing van nieuwe technieken.

Een belangrijke uitbreiding in de Wiv 2017 is de wettelijke zorgplicht die de diensten hebben voor de kwaliteit van de gegevensverwerking (artikel 24 van de Wiv 2017). Deze zorgplicht betreft ook de door de diensten gebruikte algoritmen en modellen. De nieuw opgerichte ICT-unit zal in het toezicht hierop een belangrijke rol spelen. Binnen deze unit is kennis ondergebracht van de werkprocessen van de beide diensten, van de technische middelen die daar worden toegepast, maar ook meer algemeen van data-analyseprocessen en cyber- en internettechnologie.[170]

Autoriteit Financiële Markten

De Autoriteit Financiële Markten (AFM) is een onafhankelijke gedragstoezichthouder die zich sterk maakt voor eerlijke en transparante financiële markten, zodat het publiek, het bedrijfsleven en de overheid vertrouwen hebben in de financiële markten.[171] Door technologische ontwikkelingen veranderen ook financiële markten en financiële ondernemingen, onder meer door internationalisering en digitalisering. Een speerpunt in de agenda voor 2018 van de AFM is meer te focussen op technologie en data in haar toezicht, en op de risico's die technologie binnen de financiële sector met zich meebrengt (AFM, 2018a).

Sinds begin 2016 heeft de AFM een programma Innovatie & Fintech. Dat richt zich op het ondersteunen van technologische innovatie in de financiële sector, voor zover deze bijdraagt aan duurzaam financieel welzijn in Nederland (AFM, 2017a). De AFM heeft in 2017 meermaals gewaarschuwd voor de hype rondom Initial Coin Offerings (ICO's) en crypto's, omdat deze producten grotendeels buiten toezicht vallen, de koersen schommelen, en de markt kwetsbaar is voor fraude, witwassen en koersmanipulatie (AFM, 2017b). Begin 2018 waarschuwde de AFM voor de *gamification* van financiële producten. Het gaat hier om een trend waarbij vaak zeer risicovolle financiële producten worden aangeboden met behulp van agressieve verleidingstechnieken, die ook gebruikt worden in de online *gaming*- en gokindustrie. Daarbij richten aanbieders zich ook op jongeren, bijvoorbeeld door gratis demo's aan te bieden of via beroemdheden die een product aanprijzen (De Waard & Haegens, 2018). In 2018 zet de AFM nadrukkelijker in op datagedreven toezicht om consumenten en beleggers beter te beschermen tegen risicovolle financiële producten, malafide praktijken en marktmisbruik (AFM, 2018b).

Agentschap Telecom

Agentschap Telecom (AT), onderdeel van het ministerie van EZK, is zowel uitvoerder als toezichthouder van wet- en regelgeving op gebied van

170 Idem.
171 Zie: https://www.afm.nl/nl-nl/over-afm

telecommunicatie en waarborgt de beschikbaarheid en betrouwbaarheid van de IT- en communicatienetwerken in Nederland door onderzoek uit te voeren en ontwikkelingen in de gaten te houden.[172] Zo is het AT toezichthouder op het afsprakenstelsel elektronische toegangsdiensten (ETD-stelsel) en zal het per mei 2018 ook optreden als toezichthouder van de Wet Cybersecurity voor de EZK-domeinen energie en telecommunicatie.[173]

Gezien de technologische ontwikkelingen, zet het AT zich in voor de veiligheid van het gebruik van de digitale infrastructuur. Een nieuwe uitdaging die geïdentificeerd is door het AT is de waarborging van digitaal vertrouwen. Als nieuwe taak houdt het AT sinds 2016 toezicht op de veiligheid en betrouwbaarheid van elektronische vertrouwensdiensten, zoals elektronische handtekeningen, elektronische zegels, digitale bezorgdiensten, of de authenticatie van websites. Deze elektronische vertrouwensdiensten leveren een belangrijke bijdrage aan een betrouwbare digitale samenleving (Agentschap Telecom, 2017).

Verder is het AT in gesprek met BZK over de inrichting van toezicht onder de Wet Digitale Overheid, die in januari 2019 zou moeten ingaan, op de werking, veiligheid en betrouwbaarheid van het stelsel van elektronische identiteiten, waaronder eHerkenning (inlogmiddel voor ondernemers voor interactie met de overheid) en DigiD (het inlogmiddel voor burgers), aldus het AT. Ten slotte pleit het AT voor meer bevoegdheden onder de Radioapparatenrichtlijn op het gebied van de betrouwbaarheid van de beveiligingssoftware van IoT-apparaten. In de Roadmap Digitaal veilige hard- en software (EZK 2018b) geeft het kabinet aan te onderzoeken hoe dit valt te realiseren.

Het AT is ook samenwerkingsverbanden aangegaan met het Nationaal Cyber Security Centrum en met het Digital Trust Centre. Daarnaast heeft het AT een jarenlange actieve samenwerking met de ACM; daarmee ontstaan steeds meer raakvlakken op het gebied van digitalisering en cyber (met name door de digitalisering van de telecommunicatie). Verder is de capaciteit van het AT uitgebreid voor elektrische diensten en de Cybersecuritywet.[174]

Commissariaat voor de media

Het Commissariaat voor de media (CvdM) houdt onder andere toezicht op de naleving van de Mediawet 2008, waarmee het Commissariaat de onafhankelijkheid,

172 Zie: https://www.agentschaptelecom.nl/over-agentschap-telecom/organisatie

173 Het ETD-stelsel is een afsprakenstelsel waarin verschillende aanbieders van authentificatiemiddelen en -diensten, zoals eHerkenning, participeren. Het zorgt ervoor dat publieke en private organisaties veilige en gebruiksvriendelijke toegang tot digitale dienstverlening kunnen garanderen.

174 In totaal betreft de formatie voor eIDAS en ETD ongeveer 13 fte. Zodra het toezicht op grond van de Cybersecuritywet structureel van aard is, kan dit doorgroeien naar plusminus 25 tot 30 fte.

pluriformiteit en toegankelijkheid van het media-aanbod beschermt.[175] Voor 2018 heeft het Commissariaat in zijn toezichtsbrief 2018 twee strategische thema's benoemd:

1. **het online domein**;
   Toezicht op het online domein vormde ook in 2017 een aandachtspunt en zal in 2018 steeds meer integraal onderdeel worden van het reguliere toezicht. Daarbij let het Commissariaat op de pluriformiteit en onafhankelijkheid van het online media-aanbod. Het verkende bijvoorbeeld samen met de ACM de digitalisering van nieuws (CvdM & ACM, 2018). Daarin constateren de toezichthouders dat Nederland nu nog weinig last heeft van de verspreiding van desinformatie, maar dat de impact daarvan wel serieus genomen moet worden. CvdM en ACM verkennen daarom nu al mogelijke maatregelen, zoals het investeren in voldoende en divers aanbod van kwaliteitsnieuws. Een ander belangrijk thema in het online domein is het verhogen van transparantie over commerciële beïnvloeding. In 2017 lag de focus op zelfregulering (zie oa CvdM 2017a).[176] Het Commissariaat heeft eind 2017 in samenwerking met een groep Youtubers een code tot stand gebracht, met afspraken die moet leiden tot meer transparantie over reclame in video's (CvdM, 2017b). In 2018 zal het CvdM de werking van deze code monitoren.

2. **de onafhankelijkheid van het media-aanbod**.
   Het Commissariaat monitort de onafhankelijkheid van het media-aanbod. Omdat online media steeds meer groeien, moet net als in traditionele media duidelijk zijn wanneer er sprake is van commerciële of politieke beïnvloeding. Volgens het Commissariaat moeten media-instellingen zo veel mogelijk hun eigen verantwoordelijkheid nemen door de governance en interne beheersing van hun organisatie goed te organiseren (CvdM, 2017a). Op 1 januari 2018 zijn de beleidsregels op dit vlak van kracht en het monitoren daarvan vormt een belangrijk aandachtsgebied in het toezicht van Commissariaat in 2018. Tot slot werkt het Commissariaat met diverse andere toezichthouders samen – de ACM, de AP, het AT en de Stichting Reclame Code Commissie – om effectief toezicht te bevorderen (CvdM, 2017c; CvdM, 2017d).

175 Zie: http://wetten.overheid.nl/BWBR0025028/2017-02-01

176 Videodiensten vallen nu vaak buiten de kaders van de Mediawet. Daar komt waarschijnlijk veranderingin als de nieuwe Europese Richtlijn Audiovisuele Mediadiensten in werking treedt. Dan heeft het Commissariaat ook meer mogelijkheden om online videodiensten aan te spreken op vermenging van redactie en commercie (Toezichtsbrief 2017 CvdM).

Tabel 19 Overzicht ontwikkelingen toezichthouders, op hoofdlijnen (periode 1 januari 2017 - 30 juni 2018)

Wie/wat	Technologie	Issue	Actie
AP	Digitalisering	Privacy, gegevensbescherming	Toezicht gegevensverwerking overheid en bedrijfsleven: uitbreiding van mandaat en capaciteit, toezicht op AVG
ACM	Digitalisering, platformen	Privacy, autonomie, machtsverhoudingen	Macht internetaanbieders, digitale economie, netneutraliteitswet-geving; oprichting team digitale mededinging
CRvdM	Digitalisering	Mensenrechten (speciale aandacht discriminatie), inclusie	Advies Generieke digitale infrastructuur
CTIVD	Digitalisering	Privacy, veiligheid	Toezicht op veiligheidsdiensten; veranderd mandaat n.a.v. invoering Wiv en uitbreiding budget
Autoriteit Financiële Markten (AFM)	Fintech, *big data* en algoritmen, persuasieve technologie	Autonomie, controle over technologie	Bijdragen aan een duurzaam financieel welzijn, waarschuwen voor cryptocurrencies en gamificatie van beleggen
Agentschap Telecom	Digitalisering, IoT	Digitaal vertrouwen, cyberveiligheid	Waarborgen van digitaal vertrouwen, betrouwbare telecommunicatie; uitgebreid mandaat en en uitbreiding capaciteit
Commissariaat voor de Media	Digitalisering	Onafhankelijk, pluriformiteit en toegankelijkheid van media-aanbod, vrijheid van informatie	Transparantie omtrent reclames: media-instellingen moeten eigen verantwoordelijkheid nemen door governance

Bron: Rathenau Instituut

Overige toezichthouders en toetsingscommissies

Het **Nationaal Cyber Security Centrum**[177] (NCSC) reageert op cyberdreigingen en incidenten en werkt aan het versterken van een veilige en weerbare digitale samenleving. Belangrijk focuspunt is de bescherming van de informatiesamenleving tegen cybercriminaliteit. In het *Cybersecuritybeeld Nederland 2017: Digitale weerbaarheid Nederland blijft achter op groeiende dreiging* (2017a) stelt het NCSC dat cyberaanvallen aantrekkelijk zijn, en de ontwikkeling van IoT ook risico's met zich meebrengt. Volgens het NCSC moet er de komende jaren geïnvesteerd blijven worden om de digitale weerbaarheid van Nederland te vergroten.

Daarnaast zet het NCSC zich in om het bewustzijn en de capaciteiten op het gebied van informatieveiligheid en privacy te versterken bij burgers, bedrijven en overheden. Zo biedt de Cybersecuritywet een kader voor de wijze waarop het NCSC met vertrouwelijke informatie moet omgaan en is de wettelijke grondslag van de taken en bevoegdheden van het NCSC vastgelegd (NCSC, 2017b).

Ook publiceerde de NCSC in 2017 ICT-beveiligingsrichtlijnen voor mobiele apps als leidraad voor het veiliger ontwikkelen, beheren en aanbieden van apps voor mobiele apparaten (NCSC, 2017c). De Cyber Security Raad (besproken in 'Agendavorming') ziet toe op de uitvoering van de Strategie van het NCSC. Ten slotte is de capaciteit van het NCSC de afgelopen jaren sterk uitgebreid (en dat zal de komende jaren zo doorgaan) en loopt het NCSC-budget al enkele jaren op. Dat zal ook tijdens de huidige kabinetsperiode het geval zijn. Een deel van de 95 miljoen euro die het kabinet voor cybersecurity heeft gereserveerd in het regeerakkoord, is voor het NCSC.

De **Nationale ombudsman** helpt burgers op weg die een probleem hebben met de overheid, en laat overheidsinstanties weten hoe zij hun dienstverlening kunnen verbeteren. Een van de thema's op de onderzoeksagenda voor 2018 is 'digitalisering'. De ombudsman stelt dat doordat de overheid in hoog tempo digitaliseert, dit invloed heeft op de relatie tussen burger en overheid en de manier waarop burger en overheid met elkaar communiceren (de Nationale ombudsman, 2018). Volgens de ombudsman moet de overheid de burger centraal stellen bij de digitalisering. Zo wordt onder andere benadrukt dat de overheid verantwoordelijkheid moet nemen om ervoor te zorgen dat de toegankelijkheid gewaarborgd blijft, zodat burgers mee kunnen blijven doen in de samenleving en niemand uitgesloten wordt. Ook geeft de ombudsman aan dat de overheid

177 Het NCSC is formeel geen toezichthouder.

oplossingsgericht en gebruiksvriendelijk moet zijn, en verantwoordelijkheid moet nemen voor de inrichting en uitvoering van het dienstverleningsproces.

Binnen het thema digitalisering onderzocht de Nationale ombudsman in 2015-2017 de digitale overheid, blauwe envelop en MijnOverheid en de digitalisering van het UWV, van de SVB, en van DUO. Geconstateerd werd dat digitalisering niet mag leiden tot verhindering van de toegang tot de overheid (de Nationale ombudsman, 2017). In de afgelopen periode richtte de ombudsman zich op een verkenning van 'datakoppeling/*big data*', waarbij de focus lag op de wijze waarop het burgerperspectief bij het gebruik van *big data* is geborgd. De organisatie onderzocht bijvoorbeeld het gebruik van digitale formulieren en de mogelijkheid om de digitale identiteit van overledenen op te heffen.

Ook komt er een onderzoek naar wat burgers mogen verwachten van de overheid als het gaat om het respecteren van privacy bij het aanvragen van voorzieningen (de Nationale ombudsman, 2018).

Het budget van de ombudsman is aanzienlijk verlaagd tijdens de kabinetten Rutte I en Rutte II. Dit jaar wordt dat effect weer ongedaan gemaakt en wordt het budget verhoogd. Er is geen sprake van extra mandaat voor de inzet op het thema digitalisering.

De **Stichting Reclame Code** (SRC) is de instantie op het gebied van zelfregulering van reclame, en is een initiatief van het adverterend bedrijfsleven. Om ervoor te zorgen dat reclame maken op verantwoorde wijze gebeurt, is de stichting actief op het gebied van proactieve dienstverlening (het stimuleren van reclamemakers om campagnes te ontwikkelen die voldoen aan de regels) enerzijds en regelgeving en klachtenprocedure anderzijds.

De Nederlandse Reclame Code bevat regels waaraan reclame moet voldoen, inclusief reclame die digitaal wordt verspreid. Zo moet reclame altijd herkenbaar zijn, mag reclame niet misleiden en niet in strijd zijn met de wet, de waarheid, de goede smaak en het fatsoen. Ook kent de Nederlandse Reclame Code bijzondere regels voor bijvoorbeeld reclame via sociale media en e-mail. De Reclame Code Commissie, een onafhankelijk klachtenorgaan, toetst aan de hand van de Nederlandse Reclame Code of reclame verantwoord is of niet. Als een partij het niet eens is met de uitspraak, kan beroep worden ingediend bij het College van Beroep. Zo heeft het College van Beroep in december 2017 naar aanleiding van een klacht een van de grote technologiebedrijven op de vingers getikt. Google stelde namelijk in een dagbladadvertentie dat de consument de instelling 'onthoud wat ik zoek op internet' kan uitzetten in de privacy portal en dat zoekopdrachten niet meer zouden worden onthouden. Google stelde deze belofte waar te maken.

Het College van Beroep heeft echter geoordeeld dat dit niet het geval is en dat consumenten niet goed geïnformeerd zijn. In werkelijkheid bestaat de mogelijkheid niet om ervoor te kiezen dat niets bewaard wordt van een zoekopdracht. Google bewaart bepaalde gegevens van de zoekopdracht ook indien is gekozen voor uitzetten. Volgens Google gaat het om gegevens die haar in staat stellen statistische trends te onderzoeken, tikfouten te voorkomen en haar diensten te optimaliseren.[178]

Geonovum is een overheidsstichting die geo-informatie van de publieke sector[179] toegankelijk maakt, standaarden daarvoor ontwikkelt en de overheid helpt geo-informatie beter te benutten. In de realisatie van de nationale geo-informatie-infrastructuur vormt Geonovum de schakel tussen beleid en uitvoering.[180]

Uit de meerjarenstrategie 2017-2020 blijkt de aandacht voor de voortgaande digitalisering en de rol van locatiegegevens daarbij. Er zijn meer gegevens beschikbaar dan ooit, het landschap van geo-informatie wordt rijker en complexer, en locatiegegevens worden steeds meer gebruikt voor profilering. De locatiedatadienstensector is wereldwijd een van de snelst groeiende sectoren, en door haar kennis en kapitaal is ze de drijvende kracht voor het ontwikkelen van geo-informatietechnologie.

In 2017 heeft Geonovum (2017a) de *Verkenning locatiegegevens en sociale platforms* uitgebracht. Ze wil zich meer richten op het delen van geo-informatie op het web door te werken aan betere vindbaarheid van publieke geodata op het web. Ook is informatie over locatie essentieel voor *smart city*-toepassingen. Real time gegevens worden gebruikt om mobiliteit te verbeteren. Volgens Geonovum is het slim inzetten van een informatievoorziening een van de manieren waarop de overheid efficiënter kan zijn in het verbeteren van de leefbaarheid, mobiliteit en veiligheid in stedelijk gebied. De stichting heeft daarvoor een set van praktische hulpmiddelen en spelregels opgesteld.[181]

In 2018 zal Geonovum de governancestructuur voor geostandaarden aanpassen, en de meerjarenplanning rond geostandaarden zal in de vorm van een meerjarenroadmap uitgebracht worden. Dit bouwt voort op de whitepaper geo-standaarden die in 2017 is uitgebracht (Geonovum, 2017b).

178 De volledige uitspraak is hier na te lezen: https://www.reclamecode.nl/webuitspraak.asp?ID=189633&acCode
179 Het gaat om informatie met een locatiecomponent, bijvoorbeeld een gebouw of een kanaal, of om sensormetingen die op een bepaalde plek zijn gedaan.
180 Zie: https://www.geonovum.nl/over-geonovum/waar-wij-voor-staan
181 Zie: https://meteninhetopenbaar.locatielab.nl/

Tabel 20 Activiteiten beleidsuitvoering, overige organisaties, op hoofdlijnen (periode 1 januari 2017 - 30 juni 2018)

Wie/wat	Technologie	Issue	Actie
NCSC	Digitalisering	Veiligheid, privacy, informatieveiligheid	Stimuleren veilige en weerbare digitale samenleving; uitbreiding budget
Nationale ombudsman	Digitale overheidsdiensten	Autonomie, menselijke waardigheid, digitale toegankelijkheid, verantwoordelijkheid	Klachten bij systemen van de digitale overheid die in de fout gaan, *big data*, digitale identiteit; verlaging budget Rutte I en Rutte II ongedaan gemaakt
Stichting Reclame Code	Digitalisering	Verantwoordelijkheid	Toezicht houden opdat reclame maken op verantwoorde wijze gebeurt
Geonovum	Geo-informatie; sensordata verordening	Toegankelijkheid, standaardisatie	Geo-informatie voor publieke sector/overheid toegankelijk maken

Bron: Rathenau Instituut

6.2 Internationaal

De **Europese Toezichthouder voor Gegevensbescherming** (EDPS) adviseert de Europese Commissie en het Europees Parlement over wetgeving en beleid met betrekking tot privacy en gegevensbescherming, en werkt samen met nationale toezichthouders om tot uniforme gegevensbescherming te komen. De EDPS-strategie 2015-2019 *Leading by example* bestaat uit drie hoofdprioriteiten:

1. '*data protection goes digital*': promoten van privacyversterkende technologieën, het bevorderen van cross-disciplinaire beleidsoplossingen en het verhogen van transparantie, gebruikerscontrole en accountability;
2. wereldwijde partnerschappen aangaan waarin
   a. dataprotectie ook een ethische dimensie krijgt;
   b. dataprotectie mainstream wordt in internationale politiek; en
   c. meer eenheid in de EU wordt bereikt;
3. een nieuw hoofdstuk in de Europese gegevensbescherming, door onder andere het implementeren van up-to-date regulering en het verhogen van accountability van EU-organisaties (EDPS, 2015).

In 2015 stelde de EDPS in het licht van deze strategie een ethische adviesgroep in om de verhouding tussen mensenrechten, digitale technologie en businessmodellen in de 21ste eeuw te verkennen.[182] In 2018 verscheen het eindrapport van de adviesgroep (EDPS 2018a). Daarin staan het debat rondom digitale ethiek en hoe technologie kan bijdragen aan menselijke waardigheid centraal. Het rapport geeft de volgende uitgangspunten:

1. de menselijke waardigheid moet onschendbaar blijven in het digitale tijdperk;
2. persoonlijkheid en persoonlijke data zijn onafscheidelijk;
3. digitale technologieën dragen als risico met zich mee het fundament van de democratie te verzwakken;
4. digitale gegevensverwerking bevordert nieuwe vormen van discriminatie zoals profilering; en
5. de 'commodificatie' van data (data wordt koopwaar) verschuift de waarde van personen naar persoonsdata.

Verder adviseerde de EDPS over diverse nieuwe wetgevingsvoorstellen van de Europese Commissie, waaronder de AVG, de ePrivacy-verordening (EDPS, 2017a; 2017b), het Schengen Informatie Systeem (EDPS, 2017c) en systemen voor politiesamenwerking (EDPS, 2017d).

Ook publiceerde de Europese toezichthouder een zogenoemde opinie over online manipulatie en persoonlijke data (ETGB, 2018b), waarin de toezichthouder aangeeft dat het huidige, complexe ecosysteem van digitale informatie het mogelijk maakt om mensen en politieke processen te manipuleren. Voor een effectieve aanpak is volgens het ETGB samenwerking nodig tussen verschillende beleidsdomeinen en toezichthouders. Het gaat om dataprotectieregelgeving, mededingingswetgeving, consumentenrecht en regelgeving op het gebied van verkiezingen.

Ten slotte begon de Europese toezichthouder in 2017 het '*Big Data & Digital Clearinghouse*', dat als doel heeft om toezichthouders uit bovengenoemde domeinen bij elkaar te brengen. Het Clearinghouse kijkt onder andere naar nepnieuws en kiezersmanipulatie, de opkomst van 'aandachtsmarkten' en de ondoorzichtigheid van algoritmen.

182 Zie: https://edps.europa.eu/sites/edp/files/publication/15-12-03_ethical_dimensions_nl.pdf

Tabel 21 Overzicht ontwikkelingen toezichthouders, internationaal, op hoofdlijnen (periode 1 januari 2017 - 30 juni 2018)

Wie/wat	Technologie	Issue	Actie
EDPS	Digitalisering (diensten die persoonlijke gegevens verwerken), *big data*	Verbreding van privacy naar autonomie, menselijke waardigheid, discriminatie, gegevensbescherming	Adviesgroep digitale ethiek, verkenning impact van digitalisering op mensenrechten, toezicht op AVG

Bron: Rathenau Instituut

6.3 Conclusie

Bij meer toezichthouders aandacht voor ethische aspecten van digitalisering
Bij vrijwel alle toezichthouders is het bewustzijn voor maatschappelijke en ethische aspecten van digitalisering toegenomen, bijvoorbeeld op het gebied van media en reclame, de financiële markten, marktmacht van platformen en grote technologiebedrijven, en digitale veiligheid. Veel toezichthouders oriënteren zich op de betekenis van digitalisering voor (nieuwe) aspecten van hun onderzoeksterrein, en hun eigen rol daarin, of op het opbouwen van nieuwe kennis of expertise. Bij sommige leidt dat tot nieuwe aandachtspunten in het toezicht, zoals bij de Autoriteit Financiële Markten, die nadrukkelijker gaat kijken naar het gebruik van data in de financiële sector.

Verder zien we in de periode 1 januari 2017 - 30 juni 2018 bij diverse toezichthouders een groter, of aangepast mandaat naar aanleiding van aangepaste of nieuwe wetgeving, en daaruit voortvloeiend, een verhoogd budget of capaciteit.

Nieuwe samenwerkingsverbanden
Doordat verschillende toezichthouders met digitalisering te maken hebben, is het ook van belang dat er afstemming plaatsvindt tussen de verschillende toezichthouders. We zien dat er ten opzichte van *Opwaarderen* meerdere nieuwe samenwerkingsverbanden ontstaan tussen toezichthouders, bijvoorbeeld tussen het Agentschap Telecom en het Commissariaat voor de Media of tussen het Agentschap Telecom en het Nationaal Cyber Security Centrum en het nieuwe Digital Trust Centre.

7 Vanuit publieke waarden vormgeven aan digitale transitie

Eigenlijk is de vraag: in wat voor samenleving willen we leven?[183]

7.1 Digitale transitie

In februari 2017 publiceerde het Rathenau Instituut naar aanleiding van de motie Gerkens het rapport *Opwaarderen* (Kool et al. 2017).[184] Dit bracht een breed spectrum aan maatschappelijke en ethische vraagstukken omtrent digitalisering in kaart. Een belangrijke conclusie was dat de huidige digitaliseringsgolf publieke waarden onder druk zet, zoals privacy, digitale veiligheid, gelijke behandeling en vrijheid van meningsuiting. Een andere conclusie was dat het governancesysteem – het geheel aan actoren en instituties dat maatschappelijke en ethische vraagstukken op dit gebied agendeert en vormgeeft – niet voldoende was voorbereid om publieke waarden in de digitale samenleving adequaat te kunnen beschermen. Het Rathenau Instituut stelde daarom dat een update, oftewel opwaardering, van dat governancesysteem noodzakelijk en urgent was om publieke waarden in de digitale samenleving adequaat te waarborgen. Die urgentie hangt direct samen met het inzicht dat het opbouwen van een adequaat governancesysteem vaak tientallen jaren kost.

Inmiddels zijn we anderhalf jaar verder (zomer 2018). Dit rapport is een update van *Opwaarderen*. Het schetst een integraal beeld van de stappen die door verschillende partijen in de periode 1 januari 2017 - 30 juni 2018 zijn gezet om het governancesysteem rondom ethische en maatschappelijke digitaliseringsvraagstukken te versterken. Een snelle update is gewenst omdat deze versterking vanuit maatschappelijk perspectief zeer relevant en urgent is. Het adequaat waarborgen van belangrijke publieke waarden in de digitale samenleving staat namelijk op het spel. In het verlengde daarvan gaat het om de vraag bovenaan deze pagina: in wat voor samenleving we willen leven? Daarmee is digitalisering tot in de kern van het democratische debat doorgedrongen.

183 Citaat afkomstig van: Ministerie van Binnenlandse Zaken (2018, 25-26) in NL DIGIbeter: Agenda Digitale Overheid

184 De motie, ingediend op 23 september 2014, verzocht de regering het Rathenau Instituut onderzoek te laten doen naar de wenselijkheid va een commissie die kan adviseren over de ethische kant van de digitalisering van de samenleving

Dat deze vraag nu prominent op de bestuurstafel is gekomen, laat zien dat digitalisering al lang niet meer verwijst naar een verzameling technologische gadgets. Ze reikt verder dan de automatisering van overheidsdiensten of het richtingloos stimuleren van innovatie. Het besef is doorgedrongen dat digitalisering leidt tot een nieuwe wereld, een nieuwe economie, een nieuwe democratie; kortom een nieuwe samenleving, die door nieuwe digitale middelen voortdurend op een verrassende wijze verandert (Van Est et al. 2018). Digitalisering wordt daarom steeds meer gezien als een transitie en het vormgeven daarvan als een opgave. Ook de Nederlandse Digitaliseringsstrategie *Nederland Digitaal* gebruikt veelvuldig de term ‘digitale transitie’ (EZK 2018a). In dit hoofdstuk zullen we aangeven hoe publieke waarden en deze opgave zich tot elkaar verhouden.

Paragraaf 7.2 vat samen hoe het governancesysteem op het terrein van maatschappelijke en ethische kwesties rondom digitalisering er momenteel (medio 2018) uitziet. De studie *Opwaarderen* signaleerde begin 2017 vijf blinde vlekken in het governancesysteem (zie figuur 4). In paragraaf 7.3 reflecteren we op de vraag, in hoeverre die vijf blinde vlekken de afgelopen twee jaar invulling hebben gekregen. Tot slot geven we in paragraaf 7.4 aan hoe de governance van maatschappelijke en ethische digitaliseringsvraagstukken de komende jaren verder versterkt kan worden. De centrale uitdaging is om de digitale transitie vanuit gedeelde publieke waarden richting te geven en zo te werken aan een ‘inclusieve’ digitale samenleving, waarin niemand wordt uitgesloten.

7.2 Opwaarderen is van start gegaan

De voorgaande hoofdstukken brachten in kaart, hoe het governancesysteem rondom maatschappelijke en ethische kwesties er medio 2018 uit ziet. Dit systeem bestaat uit vier domeinen: grond- en mensenrechten, maatschappij, wetenschap, en politiek en bestuur (agendavorming, beleidsvorming- en bepaling, en beleidsuitvoering). In deze paragraaf vatten we per domein onze bevindingen uit de voorgaande hoofdstukken samen.

Duidelijk is dat allerlei partijen in de samenleving bezig zijn met ethische en maatschappelijke digitaliseringsvraagstukken: het opwaarderen van het governancesysteem op dat terrein is van start gegaan.

7.2.1 Stand van zaken medio 2018

Grondrechten
In het domein van grond- en mensenrechten laat onze analyse zien dat de aandacht voor de betekenis van digitalisering zowel op nationaal als internationaal niveau is gegroeid. De discussie heeft zich vanuit technologisch perspectief verbreed: van aandacht voor het internet, naar een breed scala aan technologiegebieden, waaronder *big data* en Artificiële Intelligentie (AI), persuasieve technologie, robotica en internetplatformen. Dit heeft de discussie over de betekenis van digitalisering voor diverse grond- en mensenrechten verbreed. Naast privacy zijn in verband met digitalisering kwesties als vrijheid van meningsuiting, gelijke behandeling, autonomie en de bescherming van de democratie op de agenda gekomen.

In Nederland is er met name aandacht voor grondrechten en algoritmen, en voor digitalisering (waaronder persuasieve technologie en platformen) en de bescherming van de democratie. In Europa, of specifieker, de Raad van Europa, staat een breder scala aan technologieën op de agenda. Die onderzoekt onder andere de betekenis van convergerende technologieën, AI, geautomatiseerde gegevensverwerking, platformen, biomedische industrie, genomics, *big data* in de gezondheidszorg, robots, autonome wapens en hybride oorlogsvoering voor mensenrechten.

Zowel nationaal als internationaal is er nog weinig aandacht voor biometrie (gezichts- en emotieherkenning), Internet of Things (IoT), en *virtual* en *augmented reality* en mensenrechten, terwijl deze technologieën zich in snel tempo ontwikkelen.

Maatschappelijke organisaties en debat
Begin 2017 was er in het publieke debat vooral aandacht voor privacy en digitale veiligheid. Ook in het afgelopen anderhalf jaar waren dit belangrijke thema's. Zo heeft het referendum over de Wet inlichtingen- en veiligheidsdiensten (Wiv) in maart 2018 de gemoederen van de media en burgerrechtenorganisaties flink beziggehouden. Burgerrechtenorganisaties ageerden ook tegen ander Nederlands overheidsbeleid, zoals de invoering van de Wet Computercriminaliteit III (waarmee politie mogelijkheden krijgt om andere systemen binnen te dringen (te hacken)) en het profileringssysteem SyRi (dat de overheid inzet om fraude op te sporen).

Het maatschappelijk debat heeft zich de afgelopen anderhalf jaar ook verbreed, blijkt uit onze analyse. Er zijn nieuwe technologiegebieden, zoals *big data*, algoritmen en AI, op de agenda gekomen, en daarmee ook nieuwe maatschappelijke en ethische kwesties. Maatschappelijke organisaties vragen nu

aandacht voor de mogelijke nadelige effecten van profilering. Ze kaarten kwesties aan als inzicht in en toetsing van algoritmen (controle over technologie), en de mogelijk discriminerende of uitsluitende werking van algoritmen. Een aantal organisaties maakte mensenrechten en digitalisering tot nieuw speerpunt binnen hun organisatie, zoals Amnesty International. Bij koepelorganisaties voor het bedrijfsleven groeit voorzichtig de aandacht voor ethiek en digitalisering.

In de onderzochte periode 1 januari 2017 - 30 juni 2018 speelden de media een belangrijke agenderende rol. Door de vermeende Russische inmenging in de Amerikaanse presidentsverkiezingen in november 2016 en het Cambridge Analytica-schandaal, besteedden de media veel aandacht aan de macht van technologiebedrijven en de rol van hun platformen bij het verspreiden van desinformatie. Binnen de academische gemeenschap was al langer aandacht voor het bewust beïnvloeden van gedrag via informatietechnologie, zogenaamde persuasieve technologie (cf. Van 't Hof et al. 2012). Het Cambridge-Analytica-schandaal bracht de relevantie van dit onderwerp voor het eerst onder de aandacht van een breed publiek.

Ook was er aandacht voor de impact van digitale technologie op de gezondheid van mensen en het verslavende karakter van sociale media. Deze twee kwesties worden niet aangekaart door Nederlandse maatschappelijke organisaties. Ook komt er nauwelijks discussie op gang over *virtual* en *augmented reality* en biometrie (uitgezonderd de aandacht voor biometrische toepassingen in het paspoort), terwijl toepassingen op het vlak van gezichtsherkenning zich in snel tempo ontwikkelen en al breed toepassing vinden in de maatschappij.

Bestuur en politiek: agendavorming

Sinds begin 2017 vragen meer adviesraden om aandacht voor de betekenis van digitalisering voor de samenleving. Diverse raden richten zich op digitalisering als geheel, en benadrukken dat als gevolg daarvan publieke waarden onder druk staan. Onze analyse laat zien dat er in 2018 ook advies komt over digitalisering met aandacht voor specifieke sectoren, zoals energie, mobiliteit, zorg, democratie en de media, en aandacht voor specifieke technologiegebieden, zoals AI en digitale veiligheid. De raden benadrukken de urgentie van het beschermen van publieke waarden. Ze vragen om meer sturing en regie van de overheid om digitalisering in goede banen te leiden.

Daaraan gerelateerd constateren ze dat digitalisering zorgt voor veranderende relaties tussen overheid, bedrijfsleven, maatschappelijke organisaties en burgers. Daarom benadrukken diverse raden het belang om in gesprek te gaan met de samenleving bij het vaststellen van nieuwe kaders in de digitale samenleving. Ook

vragen ze aandacht voor de grenzen van de zelfredzaamheid van burgers. Op Europees niveau vragen adviesraden vooral aandacht voor AI.

Bestuur en politiek: beleidsvorming en -bepaling
Begin 2017 was op de diverse ministeries met name aandacht voor privacy en digitale veiligheid. In de periode 1 januari 2017 - 30 juni 2018 zien we dat de aandacht voor digitalisering zowel vanuit technologisch als ethisch en maatschappelijk perspectief is versterkt en verbreed. Op de beleidsagenda staat inmiddels een breed palet aan maatschappelijke en ethische kwesties. Sinds de start van het kabinet-Rutte III in oktober 2017 zijn er diverse agenda's opgesteld, en in juni 2018 verscheen de overkoepelende Nationale Digitaliseringsstrategie (EZK 2018a). In de tweede helft van 2018 volgen naar verwachting nog diverse beleidsnota's, bijvoorbeeld op het vlak van horizontale privacy en AI in de rechtspraak.

De Nationale Digitaliseringsstrategie kent twee sporen: 1) maatschappelijke en economische kansen benutten, en 2) versterken van het fundament langs vijf speerpunten. Een van die vijf speerpunten betreft het versterken van de weerbaarheid van bedrijven en burgers. Het gaat daarbij met name om privacy en digitale veiligheid. Op dit gebied heeft het kabinet de stap gemaakt van agenda- en beleidsvorming naar beleids*bepaling*.[185] Het komt met concrete beleidsmaatregelen op het vlak van digitale veiligheid, zoals nieuwe wetsvoorstellen, het oprichten van kenniscentra of het verbeteren van samenwerking.

Een ander speerpunt van de Nationale Digitaliseringsagenda gaat over grondrechten en ethiek in het digitale tijdperk. Nieuwe thema's hierbinnen zijn sinds begin 2017 de verspreiding van desinformatie, de bescherming van democratie en de betekenis van algoritmen voor grondrechten. Binnen dit speerpunt bevindt de beleidsvorming zich in een verkennende fase. De overheid investeert met name in kennisopbouw en heeft op een breed gebied onderzoeken aangekondigd, zoals onderzoek naar de betekenis van AI en de bescherming van publieke waarden (adviesaanvraag aan de WRR), of onderzoek naar digitalisering van de democratie (adviesaanvraag aan de Raad voor het Openbaar Bestuur).

Voor het speerpunt 'een dynamische digitale data-economie' kijkt het kabinet onder andere in hoeverre huidige wettelijke kaders voldoen. De inzet is het competitief houden van markten en helderheid over de vraag, of aanpassingen in het mededingingsinstrumentarium nodig zijn. Het kabinet kondigt voor deze vraagstukken diverse onderzoeken aan. Ook hier bevindt het beleid zich in een

185 Op het gebied van privacy bestaan al lang specifieke wetgeving en diverse beleidsmaatregelen. Op 25 mei 2018 trad de Algemene verordening gegevensbescherming (AVG) in werking.

verkennende fase. Het kabinet zet verder in op zelfregulering door platforms en samenwerking tussen (lokale) overheden en platforms.

Voor de digitale data-economie ligt de beleidsbepaling voor een belangrijk deel bij de Europese Commissie. Die komt met onder meer met voorstellen over de relatie tussen bedrijven en platformen, en het leveren van digitale content. Ook voor andere onderwerpen ligt de beleidsbepaling (deels) bij de Europese Commissie. Die moderniseert namelijk diverse wettelijke kaders, en formuleert nieuwe kaders, onder meer op het vlak van gegevensbescherming, ePrivacy, audiovisuele en mediadiensten, auteursrecht, consumentenrecht en cybersecurity.

Beleidsvorming en -bepaling: Eerste en Tweede Kamer
In de Eerste en Tweede Kamer staan privacy en digitale veiligheid op de agenda. Er zijn ook nieuwe maatschappelijke thema's op de agenda gekomen, zoals controle over technologie (inzicht in algoritmen), rechtvaardigheid (discriminatie door algoritmen), autonomie (over desinformatie, politieke *microtargeting* en keuzevrijheid), en menselijke waardigheid en machtsverhoudingen (positie van deel- en klusplatformen, omstandigheden werknemers en macht van technologiebedrijven). Via rondetafelgesprekken en deskundigenbijeenkomsten bouwen beide Kamers actief kennis op rondom nieuwe maatschappelijke en ethische digitaliseringskwesties, bijvoorbeeld op het vlak van AI in de rechtspraak, data-analytics of de deel- en kluseconomie.

Beleidsuitvoering: toezichthouders
Bij vrijwel alle toezichthouders is het bewustzijn voor maatschappelijke en ethische aspecten van digitalisering toegenomen. Veel toezichthouders oriënteren zich op de betekenis van digitalisering voor (nieuwe) aspecten van hun onderzoeksterrein en hun rol daarin. Ze bouwen kennis op over nieuwe kwesties; zie bijvoorbeeld de verkenning van de Autoriteit Consument en Markt (ACM) en het Commissariaat van de Media over de digitalisering van nieuws. Bij sommige toezichthouders leidt dat tot nieuwe aandachtspunten in het toezicht, zoals bij de Autoriteit Financiële Markten (AFM) die nadrukkelijker gaat kijken naar het gebruik van data in de financiële sector.

Ook ontstaan er meer samenwerkingsverbanden tussen toezichthouders. Het kabinet heeft een dialoogsessie voor toezichthoudende instanties op het gebied van digitale veiligheid aangekondigd, om de effectiviteit van het toezicht te bevorderen. Verder zien we in de periode 1 januari 2017 – 30 juni 2018 bij diverse toezichthouders een vergroot, of aangepast mandaat naar aanleiding van aangepaste of nieuwe wetgeving, en daarmee samenhangend, meer budget of een verhoogde capaciteit.

7.2.2 Verbreding van het debat

De belangrijkste boodschap uit *Opwaarderen* is dat ‘de overheid, het bedrijfsleven en het maatschappelijk middenveld nu actie dienen te ondernemen om het governancesysteem te versterken’ (Kool et al. 2017, p12). We concluderen dat daarin de eerste stappen zijn gezet.

Het debat over maatschappelijke en ethische vraagstukken is zowel vanuit technologisch als maatschappelijk perspectief verbreed. Er staan inmiddels meer digitale technologieën op de beleidsagenda, zoals AI, platformen en persuasieve technologie. En er is meer aandacht voor maatschappelijke en ethische kwesties op het gebied van vrijheid van meningsuiting, bescherming van democratie, gelijkheid en rechtvaardigheid, en de grenzen aan de zelfredzaamheid van de burger (autonomie). Tabel 22 geeft een overzicht van de maatschappelijke en ethische die we in *Opwaarderen* identificeerden. In *Opwaarderen* stonden privacy en veiligheid op de agenda. Inmiddels zijn ook autonomie, controle over technologie, rechtvaardigheid en machtsverhoudingen op de agenda gekomen. Binnen deze thema’s zijn een aantal nieuwe onderwerpen aan de orde gekomen; deze zijn in tabel 22 vetgedrukt.

De afgelopen anderhalf jaar is het bewustzijn over maatschappelijke en ethische kwesties op het vlak van digitalisering gegroeid. Vele partijen, zoals beleidsmakers, politici, maatschappelijke organisaties, regionale en lokale overheden, beroepsverenigingen en toezichthouders, voelen het belang van het beschermen van publieke waarden. Ze oriënteren zich op de vraag wat digitalisering betekent voor hun organisatie, sector of praktijk. De centrale vraag voor deze partijen is hoe zij digitalisering in goede banen kunnen leiden. Veel partijen erkennen dat bij digitalisering het beschermen van publieke waarden en grondrechten het uitgangspunt moet zijn. Dit betekent een ommekeer in het debat over de inzet en de invloed van digitale technologieën: van een focus op technologie en de aanname dat dit vanzelf zal leiden tot maatschappelijke vooruitgang, naar een focus op de interactie tussen digitalisering en waarden. Digitalisering is daarbij enerzijds een middel om maatschappelijke uitdagingen aan te pakken, en anderzijds een ontwikkeling die publieke waarden onder druk kan zetten.

Tabel 22 Maatschappelijke en ethische vraagstukken relevant voor digitalisering. Vetgedrukt zijn onderwerpen sinds *Opwaarderen* (2017).

Thema	Maatschappelijke en ethische vraagstukken
Privacy	Gegevensbescherming, digitaal huisrecht, mentale privacy, surveillance, doelverschuiving
Autonomie	Keuzevrijheid, vrijheid van meningsuiting, manipulatie (**verspreiding van desinformatie, *microtargeting***), **bescherming democratie**, paternalisme, **vaardigheden**, **grenzen zelfredzaamheid**
Veiligheid	Informatieveiligheid, identiteitsfraude, fysieke veiligheid
Controle over technologie	Controle over en inzicht in algoritmen, verantwoordelijkheid, voorspelbaarheid
Menselijke waardigheid	Dehumanisatie, instrumentalisering, de-skilling, de-socialisatie, werkloosheid
Rechtvaardigheid	Discriminatie, uitsluiting, gelijke behandeling, stigmatisering
Machtsverhoudingen	Oneerlijke concurrentie, uitbuiting, relatie consument-bedrijf, **relatie bedrijf-platform**

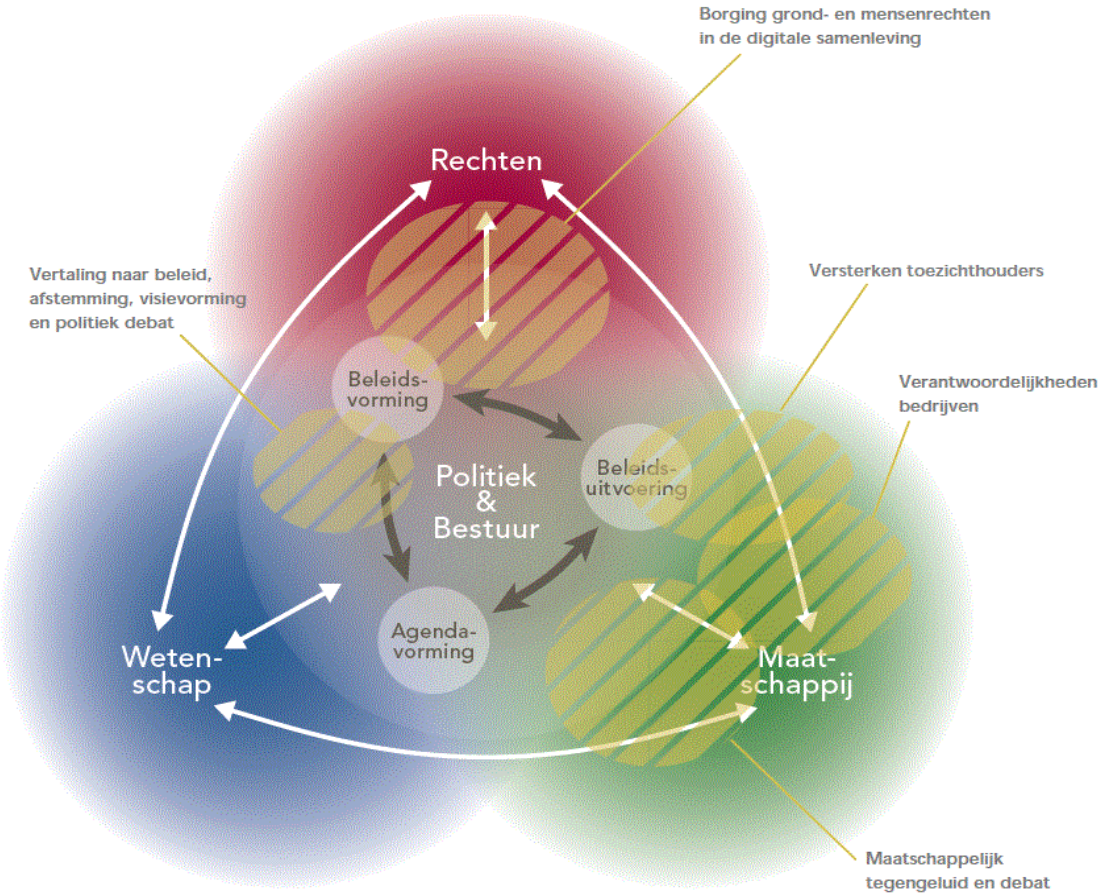
Bron: Rathenau Instituut

7.3 Blinde vlekken ten dele ingevuld

Begin 2017 constateerden we dat er vijf blinde vlekken zijn in het governancesysteem rondom ethische en maatschappelijke aspecten van digitalisering (zie figuur 4). Vanuit het inzicht dat het opbouwen van een adequaat governancesysteem een zaak van lange adem is, riep het Rathenau Instituut de overheid, het bedrijfsleven en maatschappelijke organisaties op om op de vijf genoemde terreinen snel stappen te ondernemen. Deze paragraaf brengt per blinde vlek in kaart wat er in de periode 1 januari 2017 - 30 juni 2018 in gang is gezet. Ook benoemen we voor iedere blinde vlek een aantal hiaten die nog steeds bestaan. Vanuit deze analyse komen we in paragraaf 7.4 tot vijf aanbevelingen.

Figuur 4 Vijf blinde vlekken van het governancesysteem rondom ethische en maatschappelijke aspecten van digitalisering, begin 2017

1. De vertaling van nieuwe maatschappelijke en ethische vraagstukken naar beleid. Interdepartementale afstemming en coördinatie van 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.



Bron: Rathenau Instituut (Opwaarderen, 2017)

Blinde vlek 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.

Vertaling naar beleid
Voor de thema's privacy en digitale veiligheid is de vertaling van agendering van maatschappelijke en ethische vraagstukken naar beleid op gang gekomen. Voor privacy en gegevensbescherming was dit al langer het geval. Voor digitale veiligheid en het IoT, zijn er in de periode 1 januari 2017 - 30 juni 2018 diverse beleidsagenda's gekomen met concrete beleidsmaatregelen (onder meer Nationale Cyber Security Agenda, Roadmap Digitaal veilige hard- en software en de aankomende Defensie cyberstrategie). Dat wil niet zeggen dat het beschermen van privacy en digitale veiligheid 'klaar' is: technologische en maatschappelijke ontwikkelingen leiden voortdurend tot nieuwe vraagstukken, bijvoorbeeld op het gebied van gezichtsherkenning. Dit thema staat echter niet op de beleidsagenda. Om de vertaling van nieuwe vraagstukken naar beleid te kunnen maken, is daarom een continue monitoring van ontwikkelingen nodig, om te bezien of en waar nieuwe beleidsmaatregelen nodig zijn.

De vertaling van agendering naar beleid is nog minder te zien bij nieuwe thema's, zoals de verspreiding van desinformatie of inzicht in algoritmen. Die zijn geagendeerd, maar de beleidsvorming bevindt zich in een verkennende fase. 'Grondrechten en ethiek in het digitale tijdperk' is weliswaar een speerpunt binnen de Nationale Digitaliseringsstrategie, maar die benoemt nog geen concrete beleidsmaatregelen. Het kabinet investeert momenteel met name via onderzoek in de noodzakelijke kennisopbouw. Daarbij merken we op dat in het najaar 2018 nog diverse beleidsnota's zullen verschijnen.

Voor andere onderwerpen ligt de vertaling van agendering naar beleid vooral bij de Europese Commissie. Deze moderniseert namelijk diverse wettelijke kaders, bijvoorbeeld voor privacy, auteursrecht en het consumentenrecht. De Commissie komt ook met nieuwe beleidskaders, onder meer op het vlak van illegale content en competitieve data-economie. Dat vraagt van Nederland om een tijdige vertaling van agendering naar beleid, om de Nederlandse inbreng te bepalen.

Tot slot staan diverse relevante thema's nog nauwelijks op de beleidsagenda, zoals gezichtsherkenning, *virtual* en *augmented reality* en de mogelijke gezondheidseffecten van digitale technologie. Met name gezichtsherkenning vindt snel breed toepassing in de maatschappij; deze technologie roept urgente fundamentele vragen op over onder andere privacy.

Coördinatie en afstemming beleid
Begin 2017 zagen we dat de vertaling van ethische en maatschappelijke digitaliseringsvraagstukken naar een coherent en domeinoverstijgend beleid moeizaam verliep. Beleidsdiscussies over deze vraagstukken waren vaak incident-gedreven. In *Opwaarderen* stelden we daarom voor om een overkoepelende kabinetsvisie op te stellen over de governance van maatschappelijke en ethische kwesties rondom digitalisering.

Met de Nationale Digitaliseringsstrategie van het kabinet ligt er nu een overkoepelende agenda op het gebied van digitalisering. Maatschappelijke en ethische aspecten vormen daar een onderdeel van, bijvoorbeeld met de speerpunten ‘grondrechten en ethiek in het digitale tijdperk’, ‘dynamische digitale economie’ en ‘weerbaarheid van burgers en organisaties versterken’. Ook is er medio 2018 een interdepartementale werkgroep opgericht die zich zal buigen over maatschappelijke en ethische digitaliseringsvraagstukken. Op dit vlak is er dus meer afstemming en coördinatie binnen de overheid gekomen. Tegelijkertijd is het beleid nog overwegend reactief, en wordt het met name aangejaagd door incidenten als het Cambridge Analytica-schandaal en de vermeende Russische inmenging in de Amerikaanse presidentsverkiezingen.

Coördinatie en afstemming politiek
Ook in de Eerste en Tweede Kamer is de aandacht voor maatschappelijke en ethische kwesties gegroeid, gezien de ingediende Kamervragen en moties (zie bijlage 1). Er bestaat behoefte aan overkoepelend inzicht in wat digitalisering betekent voor de bescherming van publieke waarden; zie bijvoorbeeld de (aangehouden) motie van het Eerste Kamerlid Duthler over de vraag ‘of en op welke wijze het proces van digitale transformatie nadere normering behoeft’ (Kamerstukken I 2017-2018, 34 775 VI, V), en de motie van de Tweede Kamerleden Van Dam en Van der Molen waarin de regering wordt verzocht om tot een ‘waardengedreven benadering van digitalisering te komen’ en de Kamer hierover te informeren en de ‘gelegenheid te geven bij deze waardenontwikkeling betrokken te raken’ (Kamerstukken 2017-2018 32761, nr 120).

Vanuit het kabinet is er in juni 2018 met de Nationale Digitaliseringsstrategie (EZK 2018a) een overkoepelende beleidsagenda gekomen. In verband daarmee is er op 20 september 2018 een algemeen overleg in de Tweede Kamer over digitalisering. Dit vindt plaats binnen de Vaste Commissie Economische Zaken en Klimaat. De Agenda Digitale Overheid (NLDigibeter) zal waarschijnlijk binnen de Vaste Commissie Binnenlandse Zaken worden besproken. Ook de Eerste Kamer bespreekt diverse maatschappelijke en ethische aspecten van digitalisering binnen de vaste Kamercommissies.

Er is daarmee in beide Kamers nog geen plek waar op een overkoepelende, domeinoverstijgende manier maatschappelijke en ethische digitaliseringskwesties kunnen worden besproken.

Blinde vlek 2:
Borging van grond- en mensenrechten in de digitale samenleving.
Uit onze analyse blijkt dat het kabinet op verschillende terreinen de betekenis van digitalisering voor de waarborging van grondrechten verkent. Het ministerie van BZK kijkt met name naar algoritmen en grondrechten, en de betekenis van digitalisering voor de democratie. De invulling van deze blinde vlek is daarmee op gang gekomen. Tegelijkertijd is duidelijk dat het waarborgen van grond- en mensenrechten, en eventuele aanpassingen daarvan, een langetermijnontwikkeling is. Ook de komende jaren zal op dit onderwerp inzet van het kabinet nodig zijn.

Algoritmen en de bescherming van democratie zijn niet de enige onderwerpen die om aandacht vragen. Bij de Raad van Europa is op dit moment een brede oriëntatie te zien op nieuwe technologiegebieden en maatschappelijke en ethische kwesties. In Europa is de Raad van Europa leidend voor het verkennen en vormgeven van de betekenis van nieuwe technologie voor grondrechten. Ook voor Nederland is een dergelijke brede oriëntatie belangrijk, en het is daarom van belang de aandacht voor digitalisering niet te beperken tot de rol van algoritmen of AI.

Blinde vlek 3:
Versterken van toezichthouders en zorgen voor onderlinge afstemming tussen toezichthouders.
De aandacht voor maatschappelijke en ethische aspecten van digitalisering bij toezichthouders is toegenomen. Bij diverse toezichthouders zijn het mandaat en budget vergroot. Ook wordt er geïnvesteerd in de opbouw van expertise en samenwerking met andere toezichthouders. Dit zijn belangrijke ontwikkelingen voor het versterken van het governancesysteem. De komende jaren zal moeten blijken of dit ook in de praktijk leidt tot sterke toezichthouders die handhavend kunnen optreden.

Blinde vlek 4:
Nieuwe verantwoordelijkheden van ontwikkelaars van digitale diensten en producten.
In de onderzochte periode 1 januari 2017 - 30 juni 2018 ging er bij diverse koepel- en brancheorganisaties voor het bedrijfsleven veel aandacht uit naar de invoering van de Algemene verordening gegevensbescherming (AVG). Diverse organisaties kwamen met tools om bedrijven te helpen bij de voorbereidingen op de nieuwe wet. Verder komt er voorzichtig een oriëntatie op ethische vraagstukken op gang, bijvoorbeeld op ethische codes en richtlijnen voor ontwikkelaars van o.a. robotica

en AI. Voor andere thema's, zoals controle over technologie (inzicht in algoritmen), autonomie (persuasieve technologie) en rechtvaardigheid, of voor trends, zoals gezichtsherkenning en *virtual* en *augmented reality* is nog weinig aandacht van het bedrijfsleven zichtbaar.

Onze analyse laat zien dat de druk vanuit maatschappij, beleid en politiek op het bedrijfsleven toeneemt om diens maatschappelijke verantwoordelijkheid op dit vlak te nemen. Dit zagen we de afgelopen jaren met name op het gebied van digitale veiligheid en IoT en rondom het Cambridge Analytica schandaal. In Nederland zoeken beleidsmakers naar mogelijkheden om ontwikkelaars meer verantwoordelijkheden te laten nemen. De AVG verplicht ontwikkelaars bijvoorbeeld tot privacy-by-design. Op het gebied van digitale veiligheid wil Nederland fabrikanten van consumentenelektronica verplichten tot veiligheidsupdates.

Ook rondom de deel- en kluseconomie is de vraag van verantwoordelijkheden van platformen prominent op de beleidsagenda gekomen. Cruciaal daarbij is dat er meer helderheid komt over de rol van platformen. Eind 2017 maakte het Europese Hof van Justitie eindelijk duidelijk welke verantwoordelijkheden een platform als Uber heeft met betrekking tot taxidiensten.[186]

Op andere gebieden, bijvoorbeeld bij het tegengaan van de verspreiding van desinformatie, kijkt het kabinet eerst naar zelfregulering door het bedrijfsleven. De grote internetplatformen zetten, naar aanleiding van publieke controversen of verzoeken van toezichthouders, hierin voorzichtig enkele stappen.

Het invullen van deze blinde vlek is beperkt op gang gekomen. Het ontbreekt momenteel aan een proactieve houding vanuit het bedrijfsleven om publieke waarden te waarborgen. De roep vanuit politiek en maatschappij om deze verantwoordelijkheid te nemen neemt toe. Er worden diverse wetsvoorstellen voorbereid om op dit vlak wettelijke verplichtingen voor het bedrijfsleven op te nemen. Hierbij is een zorgvuldige afweging van belang van welke verantwoordelijkheden, en op welke manier, al dan niet bij het bedrijfsleven neergelegd kunnen worden. Nu speelt bijvoorbeeld de vraag welke rol socialemediaplatformen hebben bij het snel verwijderen van haatzaaiende content, en materiaal dat mogelijk het auteursrecht schendt. De zorg bestaat echter dat internetbedrijven uit angst voor aansprakelijkheid bepalen welke content wel en niet online mag worden geplaatst, en dat dit de vrijheid van meningsuiting zal beperken.

186 Het Europese Hof van Justitie oordeelde dat de dienst die Uber aanbiedt via de app een vervoersdienst is in de zin van het EU-recht, en geen digitale dienst. Het betekent dat de EU-lidstaten nationaal mogen bepalen onder welke voorwaarden deze dienst mag worden verleend. De zaak werd door Spaanse taxichauffeurs aangespannen.

Blinde vlek 5:
Organiseren van maatschappelijk tegengeluid: versterken maatschappelijk middenveld, kennis en vaardigheden van burgers en maatschappelijk debat over digitalisering.

In *Opwaarderen* zagen we beperkt maatschappelijke discussie over de maatschappelijke en ethische betekenis van de digitaliserende samenleving. Het versterken van technologisch burgerschap, onder meer via maatschappelijke dialoog en stimuleren van digitale vaardigheden, vormde daarom een van de aanbevelingen. Technologisch burgerschap houdt in dat burgers begrip hebben van nieuwe technologie en de vaardigheden om deze te gebruiken, grip hebben op de werking en effecten van digitale technologie op henzelf en de samenleving, en kunnen deelnemen aan democratisch debat en politieke besluitvorming over technologie (Van Est 2016).

Grenzen aan digitale geletterdheid
In de periode 2017-2018 zien we groeiende aandacht voor digitale geletterdheid, digitale vaardigheden en weerbaarheid. Zo wordt er gewerkt aan een nieuw curriculum voor basis- en middelbare scholen, met aandacht voor digitalisering, en verschijnen in het najaar van 2018 de plannen voor mediawijsheid. In de Nationale Digitaliseringsstrategie is er binnen het speerpunt ‘Ander werk, nieuwe vaardigheden en levenslang leren’ aandacht voor de (digitale) vaardigheden. Tegelijkertijd is de aandacht gegroeid voor grenzen aan de zelfredzaamheid van de burger. Diverse adviesraden, de Nationale ombudsman, het ministerie van BZK en uitvoeringsorganisaties als UWV en ICTU, vragen daar aandacht voor. Het uitgangspunt is niet meer per definitie 100% digitaal: het is belangrijk dat er een analoog kanaal beschikbaar is en er wordt meer gedacht vanuit het faciliteren van burgers. Ook in de zorg waarschuwen organisaties voor de grenzen van de zelfredzaamheid (Pluut & De Jong 2018; Niezen & Verhoef 2018).

Verbreding maatschappelijk debat
Op het gebied van betrokkenheid bij het democratisch debat en politieke besluitvorming, is in de periode 1 januari 2017 - 30 juni 2018 op deelonderwerpen veel gebeurd. Burgers en maatschappelijke organisaties lieten nadrukkelijk van zich horen. Vijf studenten wisten een referendum af te dwingen over de Wiv, dat leidde tot een zeer actief publiek debat. Maatschappelijke organisaties reageren met diverse rechterlijke procedures op overheidsbeleid. Privacy, digitale veiligheid, profilering (denk aan de rechtszaak tegen het overheidssysteem SyRi) en inzicht in en controle over technologie zijn daarbij belangrijke thema’s.

Vooral de media spelen in de onderzochte periode een belangrijke rol bij het onder de aandacht brengen bij een breed publiek van kwesties als autonomie,

machtsverhoudingen of gezondheidseffecten. Met name het Cambridge Analytica schandaal heeft de relatie tussen digitalisering, democratie, media en burgerschap – en dus technologisch burgerschap – hoog op de publieke en politieke agenda gezet. Daarmee is bij veel partijen het besef doorgedrongen dat technologisch burgerschap een absolute voorwaarde is geworden voor een gezonde democratie, en ook dat er op dat gebied nog veel moet gebeuren.

7.4 Aanbevelingen

Uit dit rapport blijkt dat de laatste twee jaar bij veel partijen het besef sterk is gegroeid dat de samenleving met digitalisering voor een transitieopgave van formaat staat, met positieve en negatieve aspecten. Dit transitieperspectief betekent veel voor de governance van maatschappelijke en ethische digitaliseringsvraagstukken, omdat het de cruciale vraag op tafel legt: in welke digitale samenleving willen we leven? Om die vraag te kunnen adresseren, is een integrale innovatie-aanpak nodig, die vanuit publieke waarden vorm en richting geeft aan de digitale transitie en dus aan onze samenleving.

De belangrijkste boodschap van het Rathenau Instituut is dan ook dat de overheid, het bedrijfsleven en het maatschappelijk middenveld verder acties moeten ondernemen om het governancesysteem te versterken om zo, vanuit publieke waarden, vorm en richting te geven aan een digitale samenleving waarin niemand wordt uitgesloten.

We benoemen hieronder vijf acties waarmee beleidsmakers, bedrijven en maatschappelijke organisaties het governancesysteem op het gebied van ethische en maatschappelijke kwesties rondom digitalisering verder kunnen versterken. De eerste actie verwijst direct naar de hierboven genoemde centrale uitdaging. De actiepunten betreffen verdere acties om de in 2017 gesignaleerde blinde vlekken binnen het governancesysteem nog beter te adresseren. Het gaat daarbij steeds om het formuleren van een concrete ambitie en de noodzaak van een langdurige inzet van middelen om de digitale transitie in goede banen te leiden.

Aanbeveling 1:
Investeer in een waardengedreven benadering van innovatie
Het is belangrijk om ethische en maatschappelijke vraagstukken niet los te zien van innovatie- of digitaliseringsprocessen. Het risico bestaat dat ‘grondrechten en ethiek in het digitale tijdperk’ als laatste paragraaf van de Nationale Digitaliseringsstrategie letterlijk het sluitstuk vormen van de digitaliseringsagenda. Om de ambities van Nederland, op onder andere het gebied van mobiliteit, zorg, onderwijs en energie, waar te maken is het van belang om een koppeling te maken met

innovatieprogramma's en ethische en maatschappelijke vraagstukken. Het realiseren van een transitie, of het antwoord op de vraag 'in welke samenleving willen we leven', veronderstelt waarden centraal te zetten en als uitgangspunt te nemen. Deze omslag van denken sluit aan bij een algemene ontwikkeling in het denken over innovatiebeleid. Daarin krijgen maatschappelijke uitdagingen een steeds belangrijkere, leidende rol om richting te geven aan innovatie; dan is sprake van een missiegedreven innovatiebeleid of doelgerichte innovatiesystemen (zie Mazzucato 2018; Frenken & Hekkert 2017).

Het Rathenau Instituut pleit daarom voor 'waardevol digitaliseren', dat bestaat uit de interactie van vijf processen van innoveren: waarderen, experimenteren, kansen grijpen, risico's verzachten en samen werken en leren (Van Est et al. 2018). Bij al die processen staat de rol van publieke waarden centraal. Bij 'waarderen' gaat het ten eerste om een verheldering van het nut en de grenzen van digitalisering vanuit publieke waarden. Daarbij gaat het om streefwaarden of innovatiedoelen (zoals kwaliteit van leven, duurzaamheid, sociale inclusie, vitale economie, efficiënte dienstverlening), en om waarden die nauw verwant zijn aan grond- en mensenrechten (zoals privacy, autonomie, veiligheid, menselijke waardigheid, controle over technologie, rechtvaardigheid en machtsverhoudingen). Ten tweede gaat het om richting geven aan technologische of sociale innovatie vanuit publieke waarden. Door ethische richtlijnen vast te stellen voor de zelfsturende auto, geeft de Duitse overheid ontwikkelaars houvast en richting aan de verdere ontwikkeling van de zelfsturende auto. In Nederland stelden de gemeenten Eindhoven en Amsterdam vier kernprincipes op om richting te geven aan de digitaliseringsprocessen in hun steden (Gemeente Eindhoven en Amsterdam, 2017). Dat betekent ook eisen stellen en randvoorwaarden bepalen, onder andere voor de interactie met het bedrijfsleven.[187] Bij 'kansen grijpen' is het belangrijk dat men oog heeft voor de mogelijkheden die digitalisering biedt en deze kansen te grijpen om maatschappelijke uitdagingen te adresseren. Om 'risico's te verzachten' is oog hebben voor de risico's van digitalisering vereist en de concrete bescherming van publieke waarden via debat, beleid en technologieontwikkeling.

Aanbeveling 2:
Kom tot een proactieve, overkoepelende agenda en activiteitenplan voor maatschappelijke en ethische aspecten van digitalisering.
Het is duidelijk dat maatschappelijke en ethische aspecten rondom digitalisering nadrukkelijk op de beleidsagenda zijn gekomen. Maar er is nog geen integraal beeld en de genomen stappen zijn nog overwegend reactief. Voor privacy en digitale veiligheid is de stap van agendavorming naar beleidsbepaling gemaakt. Voor nieuwe kwesties op de agenda – zoals de betekenis van algoritmen voor

187 Zie: https://fd.nl/economie-politiek/1207927/een-sensor-op-elke-straathoek

grondrechten, de betekenis van digitalisering voor de democratie, en persuasieve technologie – is dit nog niet het geval. Voor een sterk governancesysteem zijn ook op deze gebieden concrete, en proactieve, beleidsagenda's nodig (zoals de Roadmap Digitaal veilige hard- en software). Dat vraagt ook om aandacht voor thema's die nu nog niet of nauwelijks op de beleidsagenda staan, zoals gezichtsherkenning, *virtual* en *augmented reality* en de mogelijke gezondheidseffecten van digitale technologieën. Een proactieve agenda vereist periodieke monitoring van digitale trends en bijbehorende maatschappelijke en ethische kwesties. Een overkoepelende agenda bevat ook een visie op hoe de samenleving betrokken kan worden bij de digitale transitie (zie ook aanbeveling 5).

Aanbeveling 3:
Investeer in een sterke positie van toezichthouders
Toezichthouders vormen een cruciale schakel in de versterking van het governancesysteem van maatschappelijke en ethische digitaliseringskwesties. Toezichthouders investeren in de opbouw van expertise en samenwerking met andere toezichthouders. Ook kregen diverse toezichthouders meer taken en bevoegdheden of budget, of zijn er voorstellen in voorbereiding hiertoe, bijvoorbeeld op het gebied van digitale veiligheid en media. Het is belangrijk om te monitoren of, en in hoeverre, de nieuwe mogelijkheden van toezichthouders toereikend zijn.

De genomen acties om toezichthouders te versterken, kunnen we zien als eerste stappen. We beginnen net te begrijpen waartoe de digitale samenleving in staat is. Toezichthouders vormen als onderdeel van beleidsuitvoering de handen en voeten van het beleid, maar ook de ogen en oren. Ze hebben daardoor een agenderende functie voor beleidsmakers, bijvoorbeeld als het gaat om een toereikend mandaat of instrumentarium. Het is vanuit strategisch oogpunt daarom van belang om te blijven investeren in de mogelijkheden en capaciteiten van toezichthouders.

Bij een sterke positie van toezichthouders hoort ook de mogelijkheid om te kunnen handhaven. Er is in de afgelopen jaren meer duidelijkheid gekomen over welke juridische kaders van toepassing zijn, bijvoorbeeld op het gebied van platformen. Er liggen echter nog diverse vragen in het verschiet, bijvoorbeeld over de rol en verantwoordelijkheden van socialemediaplatformen in de nieuwsvoorziening. In de komende periode is het van belang om juridische onduidelijkheden te verhelderen.

Omdat digitalisering dwars door sectoren en juridische kaders heen loopt, vraagt digitalisering de komende jaren om intensieve samenwerking tussen verschillende toezichthouders. Verspreiding van desinformatie raakt bijvoorbeeld aan juridische kaders omtrent verwerking van gegevens, verkiezingsrecht, mededingingsrecht, mediarecht en consumentenrecht. Samenwerking zal waarschijnlijk laten zien waar

onduidelijkheden over bevoegdheden bestaan, ‘gaten’ zitten die samenwerking niet afdekken en welke juridische kaders om aanpassing vragen. Beleidsmakers moeten oog te hebben voor en inspelen op dergelijke uitkomsten.

Aanbeveling 4:
Bedrijfsleven: maak werk van maatschappelijk verantwoord digitaliseren

> *I think a big mistake we have made, looking back on this, is viewing our responsibility as just building tools, rather than viewing our whole responsibility as making sure that those tools are used for good.”*
>
> Mark Zuckerberg, CEO Facebook[188]

Onze analyse laat zien dat de toegenomen politieke en maatschappelijke sensitiviteit voor maatschappelijke en ethische digitaliseringskwesties leidt tot druk op het bedrijfsleven om deze kwesties serieus op te pakken. Tot nu toe gebeurt dat mondjesmaat. Binnen de grote technologiebedrijven is lange tijd vooral aandacht geweest voor het ontwikkelen en zo snel mogelijk uitrollen van technologie, niet voor hoe de technologie gebruikt wordt. Onder druk van de maatschappij komt daar langzaam verandering in. De hierboven vermelde uitspraak van Mark Zuckerberg, die hij deed toen hij zich in april 2018 in het Amerikaanse Congres moest verantwoorden voor onder andere het Cambridge Analytica-schandaal, geeft deze veranderende houding treffend weer.

Maatschappelijk verantwoord ondernemen op het vlak van digitalisering vereist een proactieve houding van bedrijven: het voorzien van en anticiperen op mogelijke maatschappelijke en ethische implicaties van de technologie die een bedrijf ontwikkelt. Vroegtijdig inzicht in ethische en maatschappelijke aspecten, bijvoorbeeld met behulp van *ethical impact assessments*, kan leiden tot aanpassing van het ontwerp.

De verantwoordelijkheid van bedrijven om mensenrechten te beschermen 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. Ook op andere gebieden, bijvoorbeeld ten aanzien van beveiliging of gegevensbescherming, zijn er diverse zorgplichten voor bedrijven.

Het bedrijfsleven is aan zet om deze zorgplichten in de praktijk vorm te geven. Brancheorganisaties kunnen een belangrijke rol spelen bij het geven van

188 Tijdens zijn getuigenis voor het Amerikaanse Congres op 10 april 2018.

voorlichting over de bestaande zorgplichten, en ook via gedragscodes praktische invulling geven aan internationale standaarden.

Aanbeveling 5:
Stimuleer technologisch burgerschap
De betrokkenheid van de maatschappij en burgers is een belangrijk onderdeel van het richting geven aan innovatie. Het is belangrijk dat burgers begrip hebben van mogelijkheden en risico's van nieuwe technologie, de vaardigheden hebben om daar op een adequate manier in hun leven mee om te gaan, en deel kunnen aan democratisch debat en politieke besluitvorming daarover. We noemen dat 'technologisch burgerschap' (Van Est 2016). Het blijven stimuleren van de drie genoemde elementen van technologisch burgerschap is cruciaal voor een sterk governancesysteem. Daarbij is het steeds van belang rekening te houden met de grenzen van zelfredzaamheid van burgers, en hun bereidheid om te participeren.

De huidige vernieuwing van het curriculum van het lager en voortgezet onderwijs biedt goede kansen om technologisch burgerschap een adequate plek te geven in het onderwijs. Daarbij moet men aandacht geven aan het derde element daarvan: democratische burgerparticipatie. Verder is het voor de beroepsbevolking van belang digitale vaardigheden op te doen waarmee ze ook in de toekomst kans behouden op goed werk.

Bij het vergroten van publieke betrokkenheid zijn twee zaken van belang: goede informatievoorziening en mogelijkheden tot participatie. Bij informatievoorziening spelen onafhankelijke media en onderzoeksjournalistiek een centrale rol. Vanuit democratisch oogpunt is het waarborgen daarvan in een digitale samenleving cruciaal.

'Waardengedreven innoveren' betekent innovatie vanuit gedeelde publieke waarden vorm en richting geven. Dat maakt maatschappelijke betrokkenheid en dialoog noodzakelijk bij het bepalen van de gewenste richting. Betrokkenheid is op diverse plekken in onze samenleving gewenst: projectniveau, sectorniveau (zoals zorg, energie, mobiliteit, onderwijs), en diverse bestuurlijke niveaus (nationaal, provinciaal, lokaal). We zien ook dat er op tal van plaatsen initiatieven ontplooid worden. Denk aan lokale overheden die buurtbewoners betrekken bij slimme-stad-projecten of bedrijven die werknemers betrekken bij innovaties op de werkvloer. In het kader van de onder aanbeveling 2 genoemde 'proactieve, overkoepelende agenda en activiteitenplan voor maatschappelijke en ethische aspecten van digitalisering' is het hiervoor van belang dat de nationale overheid een visie ontwikkelt op het stimuleren van technologisch burgerschap en het versterken van maatschappelijke betrokkenheid bij de digitale transitie.

7.5 Tot slot

Er is een breed besef ontstaan dat de samenleving met digitalisering voor een transitieopgave van formaat staat. Digitalisering wordt niet langer meer als slechts een ICT-vraagstuk gezien. We hebben de afgelopen jaren aan den lijve ervaren hoe digitalisering onze leefwereld, economie, democratie, kortom onze gehele samenleving beïnvloedt. Digitalisering brengt continu nieuwe ethische en maatschappelijke vragen met zich mee.

Dit blijkt uit twee voorbeelden. Gezichtsherkenning zit al standaard in de nieuwe generatie smartphones, en roept urgente vragen op over het verlies van anonimiteit en privacybescherming. Nu al trekken onze smartphone, sociale media en andere apps zo aan ons, dat er steeds meer geluiden klinken over mogelijke mentale en fysieke gezondheidseffecten. De technieken in deze digitale media worden door oud-werknemers uit Silicon Valley vergeleken met technieken in gokmachines.

Het is waarschijnlijk dat de digitalisering van de samenleving zich de komende jaren zal versnellen. *Virtual* en *augmented reality*-toepassingen vinden al hun weg naar de consumentenmarkt en andere domeinen. De verdere aanleg van 5G-netwerken zal een *boost* geven aan het Internet of Things en het real-time kunnen sturen van objecten en informatie (en ons). Dit biedt kansen voor bijvoorbeeld de energietransitie, maar roept ook vele vragen op met betrekking tot zeggenschap over data, en een eerlijke en competitieve data-economie. Wereldwijd investeren bedrijven en landen vele miljarden in kunstmatige intelligentie. Volgens sommigen zal deze AI-wedloop de toekomstige economische en militaire macht van diverse landen bepalen. Over de betekenis van deze meeslepende technologieën voor onszelf, onze relaties, en onze samenleving wordt nog nauwelijks gesproken.

Het rapport *Opwaarderen* en deze update brachten we uit naar aanleiding van de Motie Gerkens, waarin de regering wordt verzocht het Rathenau Instituut onderzoek te laten doen naar de wenselijkheid van een commissie die kan adviseren over de ethische aspecten van de digitaliserende samenleving. De motie verwijst naar het Internet of Things en naar de bredere maatschappelijke, sociaal-juridische en sociaal-psychologische effecten van digitalisering. De Eerste Kamer vermoedde dat digitalisering de samenleving voor grote uitdagingen plaatst. Het rapport *Opwaarderen*, en deze update, bevestigen dit vermoeden. Hoewel er stappen zijn ondernomen om het governancesysteem te versterken, staan publieke waarden door digitalisering nog steeds onder druk. De urgentie om daadwerkelijk vanuit een digitale transitie te gaan denken en daarbij waarden centraal te zetten om vorm en richting te geven aan een ‘inclusieve’ digitale samenleving, is groot. Ook de komende jaren vraagt dat van alle partijen om eigen verantwoordelijkheid, en samenwerking met andere partijen, zowel lokaal, regionaal als internationaal.

Literatuurlijst

Adviescommissie voor Vreemdelingenzaken (2016). *Profileren en selecteren: advies over het gebruik van profilering in de uitvoering van het vreemdelingenbeleid*. Den Haag: Adviescommissie voor Vreemdelingenzaken

AFM (2017a). *Jaarverslag 2016: Scherp toezicht in een veranderend speelveld*. Amsterdam: AFM. Online beschikbaar: https://www.afm.nl/nl-nl/verslaglegging/jaarverslag

AFM (2017b). *AFM waarschuwt voor grote risico's bij Initial Coin Offerings*. (13 november 2017). Online beschikbaar: https://www.afm.nl/nl-nl/consumenten/nieuws/2017/nov/risico-ico

AFM (2018a). *AMF Agenda 2018*. Online beschikbaar: https://www.afm.nl/nl-nl/verslaglegging/agenda

AFM (2018b). AFM *zet in 2018 vol in op data-analyse om belegger te beschermen*. (24 januari 2018). Online beschikbaar: https://www.afm.nl/nl-nl/consumenten/nieuws/2018/jan/agenda-2018

Agentschap Telecom (2017). *Staat van de Ether, 2016*. Groningen: Agentschap Telecom. Online beschikbaar: https://magazines.agentschaptelecom.nl/staatvandeether/2017/01/index

Authority of the House of Lords (2018). *AI in the UK: ready, willing and able?* London: House of Lords

Autoriteit Consument & Markt (2017). *Geen dominante marktmacht bij online video-streaming platforms* (22 augustus 2017) Online beschikbaar: https://www.acm.nl/nl/publicaties/publicatie/17573/Geen-dominante-marktmacht-bij-online-video-streaming-platforms

Autoriteit Consument & Markt (2018). *Position Paper Autoriteit Consument & Markt. Rondetafelgesprek over de marktdominantie van internet- en technologiebedrijven*. 31 januari 2018. Online beschikbaar: https://www.acm.nl/sites/default/files/documents/2018-02/positionpaper-acm-over-marktdominantie-grote-tech-bedrijven.pdf

Autoriteit Persoonsgegevens (2017a). *Agenda 2017*. Den Haag: Autoriteit Persoonsgegevens.

Autoriteit Persoonsgegevens (2017b). Adviesontwerp besluit tot wijziging van het Besluit BRP. Den Haag: Autoriteit Persoonsgegevens (21 maart 2017)

Online beschikbaar: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_wijziging_besluit_brp_sila.pdf

Autoriteit Persoonsgegevens (2017c). *Wetgevingsadvies conceptwetsvoorstel Wet gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven*. Den Haag: Autoriteit Persoonsgegevens (28 april 2017) Online beschikbaar: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_pnr.pdf

Autoriteit Persoonsgegevens (2017d). *Advies wetsvoorstel Implementatiewet herziene richtlijn betaaldiensten*. Den Haag: Autoriteit Persoonsgegevens (22 augustus 2017) Online beschikbaar: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_psd2.pdf

Autoriteit Persoonsgegevens (2017e). *Adviesverzoek concept-Cybersecuritywet*. Den Haag: Autoriteit Persoonsgegevens (25 oktober 2017) Online beschikbaar: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/z2017-04917_advies_cybersecuritywet.pdf

BEUC (2018a). *Automated decision making and Artificial Intelligence – A Consumer Perspective*. BEUC Position Paper. 20-06-2018. www.beuc.eu/publications/beuc-x-2018-058_automated_decision_making_and_artificial_intelligence.pdf

BEUC (2018b). *Plugging the gap in consumer rights. What a new deal should look like in 2018*. Brussels: BEUC. Online beschikbaar: www.beuc.eu/publications/beuc-x-2018-023_what_a_new_deal_for_consumers_should_look_like_in_2018.pdf

BEUC (2018c). *Cybersecurity Act - Consumers need mandatory security by design and by default*. Brussels: BEUC. Online beschikbaar: http://www.beuc.eu/publications/beuc-x-2018-024_cybersecurity_act_consumers_need_mandatory_security_by_design_and_by_default.pdf

BMVI (2017). *Ethics Commission Automated and Connected Driving*. Berlin: BMVI.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B, Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G.C., Steinhardt, J., Flynn, C., Ó hÉigeartaigh, S., Beard, S., Belfield, H., Farquhar, S., Lyle, C., Crootof, R., Evans, O., Page, M., Bryson, J., Yampolskiy, R. & Amodei, D. (2018). *The Malicious Use of Artificial*

Intelligence: Forecasting, Prevention, and Mitigation. Online beschikbaar: https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

Centraal Planbureau (2017). *Scientia potentia est: de opkomst van de makelaar voor alles*. Den Haag: Centraal Planbureau.

Centraal Planbureau (2018). *Risicorapportage Financiële Markten 2018*. Den Haag: Centraal Planbureau

College voor de Rechten van de Mens (2017a). *Onbeperkt stemmen - Rapportage over de toegankelijkheid van verkiezingen voor mensen met een beperking*. Utrecht: College voor de Rechten van de Mens. Online beschikbaar: https://mensenrechten.nl/publicaties/detail/37739

College voor de Rechten van de Mens (2017b). *Brief aan de minister van BZK over internetconsultatie conceptwetsvoorstel Generieke digitale infrastructuur*. Utrecht: College voor de Rechten van de Mens. Online beschikbaar: https://www.mensenrechten.nl/publicaties/detail/37468

COMEST (2017). *Report of COMEST on robotics ethics* (14 September 2017). Paris: UNESCO. Online beschikbaar: http://unescoblob.blob.core.windows.net/pdf/UploadCKEditor/REPORT%20OF%20COMEST%20ON%20ROBOTICS%20ETHICS%2014.09.17.pdf

Commissie van Ministers (2017). *Reply to Recommendation | Doc. 14432* (19 October 2017). Brussel: Commissie van Ministers. Online beschikbaar: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24236&lang=en

Cultureel Planbureau (2018). *CPB Risicorapportage Financiële Markten 2018.* Den Haag: Cultureel Planbureau.

CTIVD (2017). *Jaarverslag 2016*. Den Haag: CTIVD.

Commissariaat voor de Media (2017a). *Jaarverslag 2016*. Hilversum: CvdM. Online beschikbaar: https://jaarverslag.cvdm.nl/2016/wp-content/uploads/2017/02/Commissariaat-voor-de-Media-Jaarverslag-2016-webversie.pdf

Commissariaat voor de Media (2017b). *YouTubers ontwikkelen met hulp van Commissariaat voor de Media een code om transparanter te zijn over reclame*. (17 november 2017). Online beschikbaar: https://www.cvdm.nl/nieuws/youtubers-ontwikkelen-hulp-commissariaat-media-code-om-transparanter-reclame/

Commissariaat voor de Media (2017c). *Commissariaat voor de Media en Agentschap Telecom tekenen samenwerkingsprotocol* (6 december 2017)

Online beschikbaar: https://www.cvdm.nl/nieuws/commissariaat-voor-de-media-en-agentschap-telecom-tekenen-samenwerkingsprotocol/

Commissariaat voor de Media (2017d). *Samenwerking Stichting Reclame Code en Commissariaat voor de Media* (23 november 2017) Online beschikbaar: https://www.cvdm.nl/nieuws/samenwerking-stichting-reclame-code-en-commissariaat-media/

Commissariaat voor de Media (2017d). *Samenwerkingsprotocol Consumentenautoriteit – Commissariaat voor de Media*. Online beschikbaar: https://www.cvdm.nl/wp-content/uploads/2013/04/Samenwerkingsprotocol-ACM-en-CvdM.pdf/

Cyber Security Raad (2016). *European Foresight Cyber Security Meeting 2016. Public private academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care*. Den Haag: Cyber Security Raad. Online beschikbaar: https://www.cybersecurityraad.nl/binaries/Report%20European%20Foresight%20Cyber%20Security%202016_tcm56-102235.pdf

Cyber Security Raad (2017a). *Ieder bedrijf heeft digitale zorgplichten*. Nijmegen: Xerox/OBT. Online beschikbaar: https://www.cybersecurityraad.nl/binaries/20170405_CSR_Handreiking2017_CompleetDEFweb_tcm56-253718.pdf

Cyber Security Raad (2017b). *Naar een landelijk dekkend stelsel van informatieknooppunten*. Den Haag: Cyber Security Raad. Online beschikbaar: https://www.cybersecurityraad.nl/binaries/CSR-advies%202017%20nr.%202%20-%20Naar%20een%20landelijk%20dekkend%20stelsel%20van%20informatieknooppunten_tcm56-269317.pdf

Cyber Security Raad (2017c). *Naar een veilig verbonden digitale samenleving*. Den Haag: Cyber Security Raad. Online beschikbaar: https://www.cybersecurityraad.nl/binaries/CSR%20Advies%20IoT%20digitale%20versie%20DEF%20NED_tcm56-298518.pdf

Cyber Security Raad (2018). *'Naar een open, veilig en welvarend digitaal Nederland': Advies inzake de Nederlandse Cybersecurity Agenda (NCSA)*. Den Haag: Cyber Security Raad. Online beschikbaar: https://www.cybersecurityraad.nl/binaries/CSR_Advies_NCSA_NED_tcm107-334926.pdf

De Waard, P. & K. Haegens (2018). AFM-voorzitter: *'Financieel beleggen begint op gokken en gamen te lijken'*. (24 januari 2018) Online beschikbaar: https://www.volkskrant.nl/4561537

DH BIO (2017). *Information document concerning the DH-BIO*. Brussel: Raad van Europa. Online Beschikbaar:https://rm.coe.int/inf-2017-5-e-info-doc-dh-bio/168077c578

ECP (2018). *Artificial Intelligence: Gespreksstof en handvatten voor een evenwichtige inbedding in de samenleving*. Whitepaper. Leidschendam: ECP.

Europese Commissie (2018a). *Multi-dimensional approach to disinformation. Report of the independent High Level Group on fake news and online disinformation*. Brussels: Europese Commissie.

Europese Commissie (2018b). *Bestrijding van online-desinformatie: Commissie stelt EU-brede praktijkcode voor* (26 April 2018). Online beschikbaar: http://europa.eu/rapid/pressrelease_IP-18-3370_nl.htm.

Europese Commissie (2018c). Communication from the Commission to the European Parliament, European Council, the Council, the European Economic Social Committee and the Committee of the Regions. *Artificial Intelligence for Europe.* COM (2018) 237. 25.4.2018. Brussels: European Commission.

European Group on Ethics in Science and New Technologies (2018). *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*. Brussel: European Commission.

European Political Strategy Centre (2018). *The Age of Artificial Intelligence. Towards a European Strategy for Human-Centric Machines*. Brussel: EPSC

European Political Strategy Centre (2018). *The Age of Artificial Intelligence. Towards a European Strategy for Human-Centric Machines*. Brussels: EPSC. Online beschikbaar: https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategicnote_ai.pdf

Europese Toezichthouder voor gegevensbescherming (2015). *The EDPS Strategy 2015-2019*. Brussel: ETGB. Online beschikbaar: https://edps.europa.eu/sites/edp/files/publication/15-07-30_strategy_2015_2019_update_en.pdf

Europese Toezichthouder voor gegevensbescherming (2017a). *Recommendations on specific aspects of the proposed ePrivacy Regulation*. Brussel: ETGB. Online beschikbaar: https://edps.europa.eu/data-protection/our-

work/publications/opinions/recommendations-specific-aspects-proposed-eprivacy_en

Europese Toezichthouder voor gegevensbescherming (2017b). *Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation).* Brussel: ETGB. Online beschikbaar: https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf

Europese Toezichthouder voor gegevensbescherming (2017c). *Opinion 7/2017 on the new legal basis of the Schengen Information System*. Online beschikbaar: https://edps.europa.eu/sites/edp/files/publication/17-05-02_sis_ii_opinion_en.pdf

Europese Toezichthouder voor gegevensbescherming (2017d). *Opinion 11/2017 on the proposal for a regulation on ECRIS-TCN*. Online beschikbaar: https://edps.europa.eu/sites/edp/files/publication/17-12-12_opinion_ecris_tcn_2017_0542_en.pdf

Europese Toezichthouder voor gegevensbescherming (2018a). *Ethics Advisory Group Report 2018*. Brussel: ETGB. Online beschikbaar: https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf

Europese Toezichthouder voor gegevensbescherming (2018b). *Opinion 3/2018 on online manipulation and personal data*. Online beschikbaar: https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

FRA (2018). #Big Data: *Discrimination in data-supported decision making*. Vienna: FRA. Online beschikbaar: http://fra.europa.eu/en/publication/2018/big-data-discrimination

Freese, C. & Dekker, R. (2018). *Samen werken met robots*. Amsterdam: De Burcht

Freese, C., Dekker, R., Kool, L., Dekker, F. & Est, R. van (2018). *Robotisering en automatisering op de werkvloer – bedrijfskeuzes bij technologische innovaties*. Den Haag: Rathenau Instituut

Frenken, K., Van Waes, A., Smink, M. & Van Est, R. (2017). *Eerlijk delen - Waarborgen van publieke belangen in de deeleconomie en de kluseconomie*. Den Haag, Rathenau Instituut.

Gemeente Eindhoven en Amsterdam (2017). ‘Spelregels voor de digitale infrastructuur in de stad’. Brief wethouders Depla en Ollongren. Eindhoven/Amsterdam.

Geonovum (2017a). *Verkenning locatiegegevens en sociale platforms*. Amersfoort: Geonovum. Online beschikbaar

:https://www.geonovum.nl/sites/default/files/2017%20Rapport%20locatiegegevens%20en%20platforms.pdf

Geonovum (2017b). *Whitepaper Geo-standaarden*. Online beschikbaar: https://docs.geostandaarden.nl/wp/basis-wpgs-20171222/

Heck, W. (2016). *Beperking opslag van data is tegenslag voor terreurbestrijders*. In NRC. Online beschikbaar: https://www.nrc.nl/nieuws/2016/12/22/eu-hof-beperkt-opslag-van-data-tegenslag-voor-terreurbestrijders-5891446-a1537920

High Level Expert Group (2018). *A multi-dimensional approach to disinformation. Report of the independent High level Group on fake news and online disinformation*. Luxembourg : Europese Commissie.

Hof van Justitie van de Europese Unie (2017). *Asociación Profesional Élite Taxi v Uber Systems Spain SL*. Online beschikbaar: https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2017/12/European-Court-of-Justice-Uber-ruling-December-20-2017-POLITICO.pdf

IBC (2017). *Report of the IBC on big data and health*. Paris: UNESCO. Online beschikbaar: http://unesdoc.unesco.org/images/0024/002487/248724e.pdf

Kool, L., Timmer, J., Royakkers, L. & Van Est, R. (2017). *Opwaarderen. Borgen van publieke waarden in de digitale samenleving*. Den Haag: Rathenau Instituut.

Korthagen, I. & Van Keulen, I (2017). *Online meebeslissen - Lessen uit onderzoek naar digitale burgerparticipatie voor het Europees Parlement*. Den Haag: Rathenau Instituut.

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

Meulen, van der, B. & A. Rip (1998). Mediation in the Dutch science system. In: *Research Policy* 27(8) pp. 757-769.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2018a). NL DIGIbeter. Agenda Digitale Overheid. Den Haag: BZK.

Ministerie van Binnenlandse Zaken en Koninkrijksrelatie (2018b). *Digiprogramma 2018. Digitaliseren met vertrouwen*. Den Haag: BZK.

Ministerie van Buitenlandse Zaken (2018). *Mensenrechtenrapportage. Actualisering buitenlands mensenrechtenbeleid en resultaten*. Den Haag: BZ

Ministerie van Economische Zaken en Klimaat (2017). *Navigeren met wind in de zeilen. Voortgangsrapportage Bedrijvenbeleid 2017*. Den haag: Ministerie

van Economische Zaken en KlimaatMinisterie van Economische Zaken en Klimaat (2018a) *Nederlandse Digitaliseringsstrategie*. Den Haag: EZK

Ministerie van Economische Zaken en Klimaat (2018b). *Roadmap Digitaal veilige hard- en software*. Den Haag: EZK

Ministerie van Justitie en Veiligheid (2018a). *Nederlandse Cybersecurity Agenda: Nederland digitaal veilig*. Den Haag: Ministerie van Justitie en Veiligheid

Ministerie van Justitie en Veiligheid (2018b). *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming*. Den Haag: Ministerie van Justitie en Veiligheid

Ministerie van Onderwijs, Cultuur en Wetenschappen (2018). *Aanbieding brochure Doorbraakproject en rapport Berenschot Toets SIVON*. Den Haag: OCW.

Ministerie van Sociale Zaken en Werkgelegenheid (2017). *Kamerbrief Kabinetsreactie SER-verkenning 'Mens en Technologie: samen aan het werk'*. Den Haag: SZW.

Ministerie van Sociale Zaken en Werkgelegenheid (2018). *Motie van de leden Verhoeven en Buitenweg, nr 118. 8 juni 2018*. Den Haag: Ministerie van Sociale Zaken en Werkgelegenheid

Ministerie van Veiligheid en Justitie (2017). *Reactie op het ACVZ-advies: "Profileren en selecteren".* Den Haag: Ministerie van Veiligheid en Justitie

Muller, C. (2017). *Kunstmatige intelligentie - De gevolgen van kunstmatige intelligentie voor de (digitale) eengemaakte markt, de productie, consumptie, werkgelegenheid en samenleving*. Brussel: Europees Economisch en Sociaal Comité

Munnichs, G., Kouw, M., & Kool, L. (2017). *Een nooit gelopen race - Over cyberdreigingen en versterking van weerbaarheid*. Den Haag: Rathenau Instituut.

Nationaal Cyber Security Centrum (2017a). *Cybersecuritybeeld Nederland 2017*. Den Haag: NCSC. Online beschikbaar: https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2017.html

Nationaal Cyber Security Centrum (2017b). Wet gegevensverwerking en meldplicht cybersecurity. Den Haag: NCSC. Online beschikbaar: https://www.ncsc.nl/actueel/nieuwsberichten/wet-gegevensverwerking-en-meldplicht-cybersecurity.html

Nationaal Cyber Security Centrum (2017c). ICT-beveiligingsrichtlijnen voor mobiele apps. Den Haag: NCSC. Online beschikbaar:

https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-mobiele-apps.html

Nationale ombudsman (2017). *Digitalisering mag mensen niet uitsluiten*. Online beschikbaar: https://www.rathenau.nl/nl/blog/nationale-ombudsman-digitalisering-mag-mensen-niet-uitsluiten

Nationale ombudsman (2018). *Onderzoeksagenda 2018*. Online beschikbaar: https://www.nationaleombudsman.nl/system/files/bijlage/onderzoeksprogramma%202018%20DEF_0.pdf

Niezen, M. en P. Verhoef (2018). Digitale gezondheidsregie - Meer gegevens, meer grip? Den Haag: Rathenau Instituut

OESO (2018). *Tax Challenges Arising from Digitalisation: More than 110 countries agree to work towards a consensus-based solution*. Paris: OESO. Online beschikbaar: http://www.oecd.org/newsroom/tax-challenges-arising-from-digitalisation-more-than-110-countries-agree-to-work-towards-a-consensus-basedsolution.htm

Onderwijsraad (2017). *Doordacht Digitaal*. Den Haag: Drukkerij Excelsior.

OSCE (2016). *UN Human Rights Council resolution on protection of human rights on the Internet a milestone for free speech, says OSCE Representative*. Wenen: OSCE. Online beschikbaar: http://www.osce.org/fom/250656

Parlementaire Assemblee van de Raad van Europa (PACE). (2015) *Technological convergence, artificial intelligence and human rights (Motie 24 June 2015).* Brussel: PACE. Online beschikbaar: http://www.assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=21951&lang=en.

Parlementaire Assemblee van de Raad van Europa (PACE) (2017). *Recommendation 2102 Provisional version (28 April 2017) Technological convergence, artificial intelligence and human rights*. Brussel: PACE. Online beschikbaar: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23726&lang=en

Planbureau voor de Leefomgeving (2017). *Mobiliteit en elektriciteit in het digitale tijdperk. Publieke waarden onder spanning*. Den Haag: Uitgeverij PBL.

Pluut, B. & M. de Jong (2018). E-health experts: Denk niet te gemakkelijk over zelfredzaamheid. Blogserie Beschaafde Bits. Den Haag: Rathenau Instituut.

Privacy International & Article 19 (2018). *Privacy and Freedom of Expression In the Age of Artificial Intelligence*. London: Privacy International & Article 19. Online beschikbaar: https://privacyinternational.org/sites/default/files/2018-

04/Privacy%20and%20Freedom%20of%20Expression%20%20In%20the%20Age%20of%20Artificial%20Intelligence.pdf

Raad van Cultuur (2018). *Zicht op zo veel meer*. Den Haag: Raad voor Cultuur. Online beschikbaar: http://toekomst-cultuurbeleid.cultuur.nl/sectoradviezen/audiovisueel

Raad van Europa (2018). *Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*. Strasbourg: Council of Europe.

Raad van Europa (1997). *Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (Oviedo, 4.IV.1997)*. Brussel: European Treaty Series - No. 164

Raad voor de leefomgeving en infrastructuur (2015). *Verkenning technologische innovaties in de leefomgeving*. Den Haag: Raad voor de leefomgeving en infrastructuur

Raad voor de leefomgeving en infrastructuur (2017). *Technologie op waarde schatten – een handreiking*. Den Haag: Rli.

Raad voor de leefomgeving en infrastructuur (2018). *Stroomvoorziening onder digitale spanning*. Den Haag: Rli

Raad voor Volksgezondheid en Samenleving (2017). *Implementatie van e-health vraagt om durf en ruimte*. Den Haag: RVS

Rathenau Instituut & SER (2017). *Naar een verantwoorde digitale samenleving: van kwesties naar acties: Deel I, 6 december 2017*. Online beschikbaar: https://www.rathenau.nl/sites/default/files/inline-files/Verslag%20conferenties.pdf en https://www.rathenau.nl/nl/digitale-samenleving/acties-voor-een-verantwoorde-digitale-samenleving

VVD, CDA, D66 en ChristenUnie (2017). *Vertrouwen in de toekomst. Regeerakkoord 2017 – 2021*. Online beschikbaar: https://www.rijksoverheid.nl/regering/documenten/publicaties/2017/10/10/regeerakkoord-2017-vertrouwen-in-de-toekomst

SER (2015). *Werkloosheid voorkomen, beperken en goed verzekeren*. Den Haag: SER. Online beschikbaar: https://www.ser.nl/~/media/db_adviezen/2010_2019/2015/werkloosheid-voorkomen.ashx

SER (2016). *Mens en technologie. Samen aan het werk*. Den Haag: SER. Online beschikbaar: https://www.ser.nl/nl/publicaties/adviezen/2010-2019/2016/mens-technologie.aspx

Sociaal en Cultureel Planbureau (2017). *De sociale staat van Nederland 2017*. Den Haag: SCP. Online beschikbaar: https://www.scp.nl/Publicaties/Alle_publicaties/Publicaties_2017/De_sociale_staat_van_Nederland_2017

Staatscommissie parlementair stelsel (2017). *Probleemverkenning*. Den Haag: Staatscommissie. Online beschikbaar: https://www.staatscommissieparlementairstelsel.nl/opdracht-en-aanpak

Staatscommissie Thomassen (2010). *Rapport Staatscommissie Grondwet. Den Haag: Staatscommissie Grondwet*. Online beschikbaar: https://www.rijksoverheid.nl/documenten/rapporten/2010/11/11/rapport-staatscommissie-grondwet

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.

Studiegroep Informatiesamenleving en Overheid (2017). *Maak Waar*. Den Haag: Studiegroep Informatiesamenleving en Overheid. Online beschikbaar: https://www.rijksoverheid.nl/documenten/rapporten/2017/04/18/rapport-van-de-studiegroep-informatiesamenleving-en-overheid-maak-waar

UN General Assembly, Human Rights Council: resolution 20/08 adopted by the General Assembly, The promotion, protection and enjoyment of human rights on the Internet, 29 juni 2012, A/HRC/20/L.13, online beschikbaar: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A.HRC.20.L.13_en.doc

UN General Assembly, Human Rights Council: resolution 26/13 adopted by the General Assembly, The promotion, protection and enjoyment of human rights on the Internet, 20 juni 2014, A/HRC/26/L.24, online beschikbaar: https://documents-dds-ny.un.org/doc/UNDOC/LTD/G14/059/67/PDF/G1405967.pdf?OpenElement

UN General Assembly, Human Rights Council: resolution 32/13 adopted by the General Assembly, The promotion, protection and enjoyment of human rights on the Internet, 27 June 2016, A/HRC/32/L.20, online beschikbaar: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

V2_(2018). *Jaarverslag 2017*. Rotterdam: V2. Online beschikbaar: http://v2.nl/organization/annual-reports

Van Eck, B.M.A. (2018). *Geautomatiseerde ketenbesluiten en rechsbescherming. Een onderzoek naar de praktijk van geautomatiseerde ketenbesluiten over een financieel belang in relatie tot rechtsbescherming*. Tilburg: Tilburg University

Van Est, R., Timmer, J., Kool, L., Nijsingh, N., Rerimassie, V. & Stemerding, D. (2017). *Regels voor het digitale mensenpark. 'Telen' en 'temmen' van de mens via kiembaanmodificatie en persuasieve technologie*. Den Haag: Rathenau Instituut. Online beschikbaar: https://www.rathenau.nl/nl/publicatie/regels-voor-het-digitale-mensenpark

Van Est, R. & J.B.A. Gerritsen, met medewerking van L. Kool (2017). *Human rights in the robot age: Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality – Expert report written for the Committee on Culture, Science, Education and Media of the Parliamentary Assembly of the Council of Europe (PACE).* Den Haag: Rathenau Instituut

Van Est, R. (2017). *Technologisch burgerschap: dé democratische uitdaging van de eenentwintigste eeuw*. (21 december 2017) Den Haag: Rathenau Instituut. Online beschikbaar: https://www.rathenau.nl/nl/publicatie/technologisch-burgerschap-dé-democratische-uitdaging-van-de-eenentwintigste-eeuw

Van Est, R., E. de Bakker, J. van den Broek, J. Deuten, P. Diederen, I. van Keulen, I. Korthagen en H. Voncken (2018). Waardevol digitaliseren – Hoe lokale bestuurders vanuit publiek perspectief mee kunnen doen aan het 'technologiespel'. Den Haag: Rathenau Instituut.

Van Keulen, I., Korthagen, I., Diederen, P. en Van Boheemen, P. (2018). *Digitalisering van het nieuws – Online nieuwsgedrag, desinformatie en personalisatie in Nederland*. Den Haag: Rathenau Instituut

Hof, C. van 't, J. Timmer & R. van Est (red.) (2012). Voorgeprogrammeerd: Hoe het internet ons leven leidt. Den Haag: Boom Lemma uitgevers.

Vetzo, M., J. Gerards & R. Nehmelman (2018). *Algoritmes en grondrechten*. Utrecht: Universiteit Utrecht

Villani, C (2018). *For a meaningful artificial intelligence. Towards a french and european strategy*. Online beschikbaar: https://www.aiforhumanity.fr/en

VN Mensenrechtenraad (2016).*The promotion, protection and enjoyment of human rights on the Internet. 27 Juni 2016 (A/HRC/32/L.20)*. Online beschikbaar: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

Wetenschappelijke Raad voor het Regeringsbeleid (1976). *Instellingswet WRR, art. 2a (30 juni 1976).* Online beschikbaar: http://wetten.overheid.nl/BWBR0003043/1998-01-21

Wetenschappelijke Raad voor het Regeringsbeleid (2016). *Big Data in een vrije en veilige samenleving*. Den Haag: Wetenschappelijke Raad voor het

Regeringsbeleid. Online beschikbaar: https://www.wrr.nl/publicaties/rapporten/2017/04/24/weten-is-nog-geen-doen

Wetenschappelijke Raad voor het Regeringsbeleid (2017). *Weten is nog geen doen. Een realistisch perspectief op redzaamheid*. Den Haag: Wetenschappelijke Raad voor het Regeringsbeleid.Online beschikbaar: https://www.wrr.nl/publicaties/rapporten/2017/04/24/weten-is-nog-geen-doen

Widlak, A. & Peeters, R. (2018). *De digitale kooi. (On)behoorlijk bestuur door informatiearchitectuur*. Den Haag: Boombestuurskunde.

Kamerstukken

Aanhangsel Handelingen II, 2016-2017, nr. 2075

Aanhangsel Handelingen II, 2017-2018, nr. 1612

Handelingen II 2017-2018, 9

Kamerstukken I 2014-2015, CVIII, E

Kamerstukken I 2014-2015, 33 750 XIII, E

Kamerstukken I 2016-2017, 34372

Kamerstukken I 2017-2018, 34775 VI, V

Kamerstukken II 2010-2011, 31570, nr. 20

Kamerstukken II 2015-2016, 33009, nr. 16

Kamerstukken II 2016-2017, 26643 en 32761, nr. 426

Kamerstukken II 2016-2017, 32034, nr. 22

Kamerstukken II 2016-2017, 34741, nr. 2

Kamerstukken II 2017-2018, 26643 en 32761, nr. 537

Kamerstukken II 2017-2018 32761, nr. 120

Kamerstukken II 2017-2018, 32827, nr. 126

Kamerstukken II 2017-2018, 32827, nr. 127

Kamerstukken II 2017-2018, 34388, nr. G

Kamerstukken II 2017-2018, 34851, nr. 23

Kamerstukken II 2017-2018, 34861, nr.2

Kamerstukken II 2017-2018, 26643, nr. 488

Kamerstukken II 2017-2018, 26643, nr. 490

Kamerstukken II 2017-2018, 26643, nr. 496

Kamerstukken II 2017-2018, 26643, nr. 508

Kamerstukken II 2017-2018, 29023, nr. 228

Kamerstukken II 2016-2017, 33009, nr. 39

Kamerstukken II 2016-2017, 33009, nr. 42

Kamerstukken II 2017-2018, 33009, nr.47

Kamerstukken II 2017-2018, 33009, nr. 48

Kamerstukken II 2017-2018, 34588, nr. 70

Kamerstukken II 2017-2018, 34775 VI, nr. 88

Kamerstukken II 2017-2018, 34775 VII, nr. 52

Kamerstukken II 2017-2018, 34775, nr. 88

Kamerstukken II 2017-2018, 26643, nr. 527

Kamerstukken II 2017-2018, 26643, nr.529

Bijlage 1 Kamervragen en moties

Via *deskresearch* hebben we in kaart gebracht welke schriftelijke Kamervragen en moties in de periode van januari 2017 tot en met juni 2018 aandacht vroegen voor de ethische en maatschappelijke kwesties rondom de technologiegebieden die wij in de inleiding hebben besproken. We hebben de gestelde vragen en ingediende moties ingedeeld in de zeven waarden uit *Opwaarderen*: privacy, digitale veiligheid, autonomie, controle over technologie, menselijke waardigheid, rechtvaardigheid en machtsverhoudingen. Vaak hebben de vragen en moties raakvlakken met meerdere publieke waarden, maar we hebben ze bij één waarde ingedeeld (degene die het meest centraal lijkt te staan in de vragen).

Privacy – Tweede Kamer

	2018 (27 Kamervragen)
1	Het bericht dat twee derde van 150 populaire websites de privacywet overtreedt
2	Ontoegankelijkheid van Amerikaanse nieuwssites door EU regels
3	Het bericht ‘Mkb kan uitzondering op nieuwe strenge privacywet wel vergeten’
4	Het bericht ‘ABN Amro wil klantdata gebruiken voor advertenties’
5	Het bericht ‘Gegevens huisdieren en hun baasjes op straat’
6	Wetgeving voor particulier en professioneel dronegebruik
7	De Algemene verordening gegevensbescherming (AVG) en de Belastingdienst
8	Het bericht ‘Privacywet of niet, Kadaster deelt privégegevens’
9	Het bericht ‘Jouw medicijnen worden straks misschien wel door een drone gebracht’
10	Het bericht dat Meld Misdaad Anoniem gegevens doorverkoopt
11	Gebruik informatie uit het Handelsregister voor facebook-targeting
12	Het gebruik van gegevens uit het handelsregister voor direct marketing aan ZZP’ers en kleine ondernemers
13	Het bericht dat informatie van de Kamer van Koophandel gebruikt wordt voor reclamedoeleinden
14	Het bericht dat tientallen medewerkers van het Hagaziekenhuis ongeoorloofd een medisch dossier hebben ingekeken
15	Het bericht ‘Tientallen snuffelden ongeoorloofd in medisch dossier Barbie’
16	Privacyschendingen door Facebook
17	Het rapport van de CTIVD over de AIVD en het gebrek aan privacy bij informatie-uitwisseling
18	Het bericht 'Hoe de digitale halsband van Magister de privacy van schoolkinderen nekt'
19	Privacyschendingen door Facebook
20	Gestolen politie-uniformen
21	Het bericht ‘Gemeente harkt te veel persoonsgegevens binnen’
22	De veiligheid van vrouwen op het internet
23	Het sociale mediagebruik van de politie
24	Kloksystemen op basis van vingerafdrukken
25	Locatiebepalingen bij 112 meldingen
26	Het delen van persoonsgegevens van gebruikers van Valys
27	Cambridge Analytica

	2017 (34 Kamervragen)
1	Het bericht “Sollicitant niet meer vogelvrij op internet.”
2	Het gebruik van spyware in China
3	Verhandelbare spionagesoftware en de persoonlijke levenssfeer
4	Het bericht dat de AIVD en het kabinet burgers misleiden
5	Gestolen data van Übergebruikers
6	Naming and shaming op internet
7	Het bericht dat de vingerafdruk op het Nederlandse paspoort nooit wordt gecontroleerd
8	Het bericht dat bedrijven ongevraagd klantgegevens delen met Facebook
9	Een droneverbod vanwege privacy
10	Het op straat belanden van gevoelige gegevens van 1800 kwetsbare leerlingen
11	Het bericht dat op station Amsterdam Centraal slimme reclameborden worden ingezet
12	Het bericht ‘reclameborden op Amsterdam CS weten wanneer en hoelang jij kijkt’
13	Het bericht dat het project met de slimme camera’s in de haven van Rotterdam stil ligt
14	Ov-chipkaartbedrijf Translink dat de reisgegevens van honderden studenten heeft doorgegeven aan de Dienst Uitvoering Onderwijs
15	Het overdragen van sociale media data van gewone Nederlanders aan de Amerikaanse overheid, de Muslimban en de onderhandelingen over de Amerikaanse preclearance faciliteiten op Schiphol
16	Patiënten die onder druk gezet worden om bijzondere persoonsgegevens af te staan in de geestelijke gezondheidszorg
17	Het artikel ‘Dubieuze gluurcamera gewoon te koop via Amazon’
18	Het bericht dat Google gebruikersgegevens in buitenlandse datacentra moet overhandigen aan de VS
19	Het bericht dat er camera’s hangen in de kleedkamers van fitness keten ‘Fit For Free’
20	Betalen door data te delen en de verkoop van consumentendata aan bedrijven en de overheid
21	Het bericht dat er een camera in een toilet in een café is geplaatst
22	De aanbesteding van mobiele telefonie
23	Het bericht 'Privacy van leerlingen groeit scholen boven het hoofd' en het rapport 'Doordacht Digitaal' van de onderwijsraad
24	Het bericht dat Google gebruikersgegevens in buitenlandse datacentra moet overhandigen aan de VS
25	Het bericht dat er in Almelo per app gestemd kan worden
26	De verkoop van browsergegevens
27	Het toestemmingsvereiste voor de verwerking van ROM gegevens
28	Het artikel ‘Een ongeluk. 112 aan de lijn, maar waar zit je precies?’
29	Mogelijke privacy risico's in de online belastingaangifte
30	Het bericht “Consumentenbond wil Bel-me-niet-Register ook voor ex-klanten”
31	Het onderzoek van de Consumentenbond over het Bel-me-niet Register
32	Inzage in e-mails van het ministerie van Algemene Zaken inzake de Teevendeal
33	Het herkenbaar uitzenden van beelden ten behoeve van de opsporing
34	De uitspraak van de Hoge Raad dat vergaand onderzoek in smartphones privacy-rechten schendt

	2018 (8 moties)
1	Motie van de leden Van Kooten-Arissen en Hijink over privacy- en burgerrechtenorganisaties actief betrekken bij het Informatieberaad Zorg
2	Motie van het lid Van Nispen over standaardmodellen voor het vragen van toestemming voor gegevensverwerking
3	Motie van het lid Kuiken over een beter Europees privacytoezicht

4	Motie van de leden Van Raak en Arissen over een voorstel waarin de sleepnetfunctie uit de wet wordt gehaald
5	Motie van het lid Van Nispen over meer geld voor de Autoriteit Persoonsgegevens
6	Motie van de leden Verhoeven en Van Nispen over de uitvoering van de additionele taken door de AP
7	Motie van het lid Koopmans c.s. over ervaringen en voornemens inzake de AVG
8	Motie van de leden Van der Staaij en Van Toorenburg over duidelijke richtlijnen voor de functionaris gegevensbescherming
	2017 (21 moties)
1	Motie van de leden Diertens en Van den Berg over ROM-data
2	Motie van het lid Kooiman over ROM gegevens
3	Motie van het lid Arissen over een verbod op het delen van ongeëvalueerde gegevens
4	Motie van het lid Arissen over de privacy van burgers in relatie tot de Wet op de inlichtingen- en veiligheidsdiensten
4	Motie van het lid Arissen over het vrijstellen van medische informatie
5	Motie van het lid Arissen over geen gegevens verzamelen en bewaren van burgers die geen doelwit zijn van de diensten
7	Motie van het lid Özdil over geen reisgegevens van studenten meer opvragen
8	Motie van de leden Özütok en Van Engelshoven over een heldere richtlijn over welke medewerkers welke gegevens mogen inzien
9	Motie van het lid Helder over knelpunten in de privacywetgeving wegnemen
10	Motie van het lid Van Oosten over de mogelijkheden en beperkingen in de privacyregelgeving voor informatiedeling tussen professionele partijen
11	Motie van het lid Van Dam over alleen transacties via derdenrekeningen
12	Motie van het lid Van Oosten over de mogelijkheden en beperkingen in de privacyregelgeving voor informatiedeling tussen professionele partijen
13	Motie van de leden Lodders en Geurts over cameratoezicht in relatie tot de huidige capaciteit van de NVWA
14	Motie van de leden Lodders en Geurts over nog niet overgaan tot vrijwillig cameratoezicht
15	Motie van het lid De Groot over monitoren van het gebruik van camerabeelden door de NVWA
16	Motie van het lid Grashoff over camerabeelden zonder restricties ter beschikking stellen aan de NVWA
17	Motie van het lid Verhoeven over een aanvullende grondwettelijke bescherming tegen inmenging door derden
18	Motie van de leden Van Toorenburg en Kuiken over het gebruik van camerabeelden bij de opsporing van drugscriminelen
19	Motie van de leden Omtzigt en Bashir over een extern en onafhankelijk onderzoek naar databeveiliging bij de Belastingdienst
20	Motie van het lid Schouten over risico's bij uitwisseling van data met buitenlandse diensten
21	Motie van het lid Koser Kaya over gratis toegang tot relevante contactgegevens van ambtenaren

Privacy – Eerste Kamer

	2017 (1 motie)
1	Motie-Wezel (SP) c.s. over het uitsluitend verstrekken van no-hit gegevens voor opsporingsdoeleinden en de inlichtingendiensten (EK 33.542, H)

Digitale veiligheid – Tweede Kamer

	2018 (16 Kamervragen)
1	Driekwart van de 500 duizend websites van het MKB die privacygevoelige informatie verwerken is kwetsbaar voor digitale inbraak.
2	Onveilige telefoons van Samsung
3	Het bericht ‘Agentschap Telecom slaat alarm over hackbare apparaten’
4	Het bericht ‘Luchtmacht klaar voor bewapende drone’
5	De risico's die de overbelasting van de elektriciteitsvoorziening brengt voor de digitale koppositie van Nederland
6	Het bericht dat mbo- en hbo-studenten onvoldoende cybersecurity kennis en vaardigheden aanleren
7	Het bericht ‘IT-controleurs: te weinig investeringen in cyberbeveiliging’
8	Het bericht 'Gevaarlijk pedohandboek ongestoord verspreid via internet'
9	Het bericht 'Een database om miljardenfraudes te voorkomen: in het VK kan ’t wél’
10	Onlineoplichting via datingsites
11	Exportcontrole op cybersurveillancegoederen
12	De overname chipbedrijf NXP door Qualcomm
13	De aanhoudende DDoS aanvallen op Nederlandse banken en de Belastingdienst
14	DDoS-aanvallen op banken
15	Het bericht ‘Nederland is niet up-to-date’
16	De berichten ‘Spionnenjacht blokt 5G’ en ‘Arena geen proeftuin voor nieuwste generatie mobiel internet’
	2017 (27 Kamervragen)
1	Nederlanders die probeerden omstreden spionagesoftware te verkopen aan Ecuador
2	Het bericht ‘Merendeel gemeenten mailt onveilig’
3	Het bericht ‘Cybersecurity hoogleraren vrezen dat Nederland digitaal onder water komt te staan’ en het bijbehorende position paper
4	De onveiligheid van “Internet of Things” in Nederland
5	Het bericht dat de smartphones van NAVO-troepen gehackt proberen te worden
6	Het bericht ‘Fox IT houdt zeggenschap staat af’
7	Het bericht dat het bedrijf Fox-IT de zeggenschap van de staat afhoudt
8	Het feit dat er een groei van 122% is geconstateerd in varianten van ransomware
9	Het bericht dat DNB het beheer van vertrouwelijke data wil uitbesteden
10	Nationale veiligheidseisen bij aanbestedingen van cruciale communicatiediensten van de overheid
11	Het bericht dat ziekenhuizen getroffen zijn door ransomware-aanvallen
12	Het bericht dat malware mogelijk energiebedrijven kan platleggen
13	Nationale veiligheidseisen bij aanbestedingen van cruciale communicatiediensten van de overheid
14	Het bericht dat de gemeente Groningen de ICT-voorzieningen privatiseert
15	De internationale cyberaanval en de ICT van de Overheid
16	De ICT-storing in het systeem van Amadeus waardoor overal ter wereld reserveringssystemen voor de luchtvaart uitvielen
17	Het bericht dat er binnen de gehele overheid is informatieveiligheid nodig is
18	Het bericht dat bedrijven nog te weinig doen aan digitale veiligheid
19	De beveiliging van websites van Nederlandse ambassades
20	Het bericht dat de CIA kwetsbaarheden in met het internet verbonden apparaten misbruikt

21	De berichten ‘Datalekken bij gemeenten; het is een beetje een zooitje’ en ‘Organisaties worstelen met nieuwe privacy wetgeving’
22	Het bericht ‘Overheid eist invloed bij cyberbeveiliger Fox-IT’
23	Het bericht dat een Brits bedrijf het IT-beveiligingsbedrijf dat Nederlandse staatsgeheimen beveiligd heeft overgenomen
24	Russische hackers die gebruikmaken van Nederlandse server
25	Het bericht dat meerderheid van de zorgsites onbeveiligd is
26	Het onderzoek dat een meerderheid van de zorgwebsites geen veilige HTTPS-verbinding heeft
27	De verdubbeling van het aantal datalekken door ziekenhuizen

	2018 (12 moties)
1	Motie van Kuiken en Van Der Staaij over een digitaal gebiedsverbod voor haatzaaien
2	Motie van de leden Van Oosten en Buitenweg over naming and shaming bij niet verwijderen van kinderpornografie
3	Motie van het lid Van Toorenburg c.s. over internetbedrijven die zich niet committeren aan de notice-and-take-down-procedures
4	Motie van het lid Paternotte c.s. over oplossingen voor de Sigint-functie
5	Motie van het lid Van Helvert over de app WeChat
6	Motie van het lid Diks over de capaciteit voor cyberdefensie
7	Motie van het lid Buitenweg over instelling van een EU-cybersecuritywerkgroep
8	Motie van het lid Verhoeven over doorgeven van onbekende kwetsbaarheden
9	Motie van het lid Alkaya over zorgaanbieders aanwijzen als aanbieder van essentiële diensten
10	Motie van het lid Van der Lee over de screening van buitenlandse investeringen
11	Motie van het lid Paternotte c.s. over certificering van op internet aangesloten apparaten
12	Motie van de leden Kuiken en Arno Rutte over een "digitaal gebiedsverbod"
	2017 (17 moties)
1	Motie van het lid Bruins Slot c.s. over investeren in cyber
2	Motie van het lid Amhaouch c.s. over digitalisering door het brede mkb
3	Motie van het lid Arissen over een verbod op hacken
4	Motie van de leden Von Martels en Amhaouch over de risico's van cyberaanvallen
5	Motie van het lid Hijink over hacktests op IoT-apparatuur
6	Motie van het lid Diks over het in EU-verband samenbrengen van militaire expertise op het gebied van cybersecurity
7	Motie van de leden Bruins Slot en Van Engelshoven over de betrouwbaarheid en veiligheid van de Ondersteunende Software Verkiezingen
8	Motie van de leden Hijink en Verhoeven over maatregelen om consumenten te beschermen tegen slecht beveiligde apparatuur
9	Motie van het lid Verhoeven c.s. over een mandaat voor het NCSC om (semi-)publieke instellingen te helpen bij cyber security
10	Motie van de leden Buitenweg en Verhoeven over een jaarlijkse test van de vitale ICT-infrastructuur
11	Motie van het lid Krol over het proactief delen van kennis over digitale veiligheid
12	Motie van het lid Hijink over het oprichten van een digital trust centre
13	Motie van het lid Aukje de Vries c.s. over het voor eind 2017 wegwerken van onvolkomenheden op het gebied van informatiebeveiliging
14	Motie van de leden Schouten en Omtzigt over het op orde brengen van de informatiebeveiliging en het beheer van het financiële systeem van de Tweede Kamer

15	Motie van het lid Amhaouch over een adequate beveiliging van hard- en software voor het verkiezingsproces
16	Motie van het lid Van Engelshoven over bevorderen dat mensen met tweestapsidentificatie inloggen via DigiD
17	Motie van het lid Schouten over extra middelen voor de CTIVD

Digitale veiligheid – Eerste Kamer

	2018 (2 moties)
1	Motie-Strik (GroenLinks) c.s. over de instelling van een onafhankelijke toetsingscommissie (EK 34.372, J)
2	Motie-Bredenoord (D66) c.s. over de AMvB waarin misdrijven kunnen worden aangewezen waarvoor een bevoegdheid tot binnendringen in geautomatiseerde werken wordt gecreëerd (EK 34.372, I)

Autonomie – Tweede Kamer

	2018 (10 Kamervragen)
1	Het bericht ‘Populaire games overtreden gokregels’
2	Het bericht 'Medische gegevens in eigen beheer op je computer of telefoon: vanaf volgend jaar is het mogelijk'
3	Het bericht 'Gegevens miljoenen Facebook-gebruikers gestolen voor politieke reclame'
4	Beïnvloeding door buitenlandse entiteiten van democratische verkiezingen
5	Nepnieuwsbestrijders van de EU die Nederlands nieuws beoordelen maar geen Nederlands spreken
6	Nepnieuws
7	Het bericht 'Online burgerinspraak kan leiden tot teleurstelling in politici'? en het rapport van het Rathenau instituut 'Online meebeslissen'?
8	Het door ‘EU vs Disinfo’ bestempelen van journalistieke verslaggeving tot nepnieuws
9	Het bericht ‘Meer gemeenten ruilen e-mail om voor online formulier’
10	Het verdwijnen van pinautomaten en de verminderende toegankelijkheid tot contant geld
	2017 (4 Kamervragen)
1	Massasurveillance door de Oezbeekse overheid
2	Onvoldoende mobiel bereik in delen van Brabant
3	Het niet tijdig beschikbaar zijn van digitale leermiddelen
4	Het bericht dat volgens de rechter een datavrije muziekbundel niet in strijd is met netneutraliteit

	2018 (15 moties)
1	Motie van het lid Becker over een centraal informatiepunt
2	Moties van het lid Verhoeven c.s. over pleiten voor keuzevrijheid voor gebruikers
3	Gewijzigde motie van de leden Kwint en Yesilgöz-Zegerius over het opheffen van EU versus Disinfo (t.v.v. 21501-34-286)
4	Motie van het lid Westerveld over een andere strategie voor EU versus Disinfo
5	Motie van de leden Sneller en Verhoeven over een Europese strategie tegen ondermijnende desinformatie

6	Motie van het lid Yesilgöz-Zegerius over afschaffing van EU versus Disinfo
7	Motie van de leden Kwint en Leijten over het opheffen van EU versus Disinfo
8	Motie van het lid Tielen over verbeteren van digitale vaardigheden
9	Motie van het lid Den Boer over de consequenties van activeren zonder e-mailaccount
10	Motie van het lid Omtzigt over de Berichtenbox van de Belastingdienst
11	Motie van het lid Özütok over het verbeteren van de Berichtenbox
12	Motie van het lid Paternotte over 5G-uitrol in buitengebieden
13	Motie van het lid Alkaya over behoud van netneutraliteit
14	Motie van de leden Van Raan en Paternotte over nummerportabiliteit verankeren in de Bankenwet
15	Motie van het lid Leijten over een actieve keuze voor digitale post
	2017 (14 moties)
1	Motie van de leden Voortman en Recourt over toegankelijker en transparanter ingerichte internetconsultaties
2	Motie van het lid Van der Molen over uitbreiding van de reikwijdte van de richtlijn door toevoeging van social media als uitstel niet haalbaar is
3	Motie van de leden Paternotte en Ellemeet over aandringen op uitstel van besluitvorming over de reikwijdte van de richtlijn ten aanzien van social media c.q. video sharing platforms
4	Motie van de leden Van der Molen en Verhoeven over vergroting van de weerbaarheid
5	Motie van het lid Baudet over een concreet plan voor een individueel digitaal stemsysteem
6	Motie van het lid Sienot c.s. over innovatieve oplossingen voor bereikbaarheid
7	Motie van het lid Verhoeven c.s. over beïnvloeding van democratische processen door nepnieuws
8	Motie van de leden Westerveld en Van den Hul over de mediawijsheid onder senioren en volwassenen
9	Motie van de leden Ellemeet en Yesilgöz-Zegerius over onderzoek naar de staat van de Nederlandse onderzoeksjournalistiek
10	Motie van de leden Ellemeet en Yesilgöz-Zegerius over inzicht in middelen van de publieke omroep voor onderzoeksjournalistiek
11	Motie van het lid Bouwmeester c.s. over een lange termijndoel opstellen dat leidt tot een digivaardig Nederland
12	Motie van het lid Omtzigt over belastingbrieven zowel digitaal als op papier versturen
13	Motie van de leden Kuiken en Verhoeven over oneigenlijke beïnvloeding van verkiezingen
14	Motie van het lid Öztürk over een fonds voor de aanpak van nepnieuws

Controle over technologie – Tweede Kamer

	2018 (3 Kamervragen)
1	Het bericht ‘Algoritme voorspelt wie fraude pleegt bij bijstandsuitkering’
2	De berichtgeving over het proefschrift van Marlies van Eck van de Tilburg University
3	De ontwikkeling en het gebruik van ‘killer robots’
	2017 (1 Kamervraag)
1	Feitelijke vragen n.a.v. de Zembla-uitzending "Belastingdienst overtreedt willens en wetens privacywet"

	2018 (3 moties)

1	Motie van het lid Verhoeven c.s. over openbaarheid van de werking en de broncode van algoritmen en analysemethoden
2	Motie van de leden Verhoeven en Buitenweg over openbaarmaking van databestanden, algoritmes en analysemethodes van SyRI
3	Motie van het lid Buitenweg over verruimen van de mogelijkheden voor collectieve procedures bij de rechter
	2017 (0 moties)

Menselijke waardigheid – Tweede Kamer

	2018 (6 Kamervragen)
1	Het bericht 'Computer zegt nee. Hoe Saskia twintig jaar vastliep in het systeem'
2	Een vorm van slavernij bij PostNL
3	Het bericht 'Blussen? Dat doen we straks met een robot'
4	Stress veroorzakende klantbeoordelingssystemen
5	Het bericht ‘Callgirl voor Albert Heijn’
6	Misstanden met arbeidsmigranten bij distributiecentra van Albert Heijn
	2017 (0 Kamervragen)

	2018 (0 moties)
	2017 (1 motie)
1	Motie van het lid Marcouch over vergroten van de capaciteit bij de douane voor toezicht, handhaving en opsporing

Rechtvaardigheid – Tweede Kamer

	2018 (4 Kamervragen)
1	De berichten 'Debacle met digitale rechtspraak was voorzienbaar' en 'Digitalisering blijft steken'
2	Het bericht ‘Robotrechter e-Court is een groot en niet-transparant zwart gat?’
3	E-Court
4	Achterstanden bij de digitalisering van de rechtspraak
	2017 (0 Kamervragen)

	2018 (1 motie)
1	Motie van het lid Buitenweg over vormen van digitale arbitrage
	2017 (1 motie)
1	Motie van de leden Segers en Van Dam over Duitse boetewet socialmediabedrijven

Machtsverhoudingen – Tweede Kamer

	2018 (10 Kamervragen)
1	Maaltijdbezorger Deliveroo ronselt minderjarigen
2	De pakketsorteerders die via een schijnconstructie worden ingehuurd bij PostNL
3	De ongevallenverzekering voor Deliveroo bezorgers
4	Het omgaan met de mogelijkheden om deelplatforms te kunnen onderwerpen aan nationale regels
5	Validatie van 80%-norm arbeidsovereenkomst postsector
6	De mogelijkheid van een Airbnb-hypotheek
7	De gevolgen van dalende postvolumes voor de postbezorging
8	Dat Schiphol Deliveroo inzet voor bezorging aan de gate
9	16 miljard belastingontwijking van Google via Nederland
10	De uitspraak van het Europese Hof van Justitie dat Uber een taxibedrijf is
	2017 (4 Kamervragen)
1	De eenzijdige opgelegde commissieverhoging door Thuisbezorgd.nl
2	Een gemeentelijke meldplicht voor verhuur van woningen via digitale platforms
3	Het bericht dat maaltijdbezorger Deliveroo alle koeriers in loondienst gaat vervangen door (schijn)zelfstandigen
4	Het bericht dat maaltijdbezorger Deliveroo alle koeriers in loondienst gaat vervangen door (schijn)zelfstandigen

	2018 (5 moties)
1	Motie van de leden Paternotte en Wörsdörfer
2	Motie van de leden Van der Lee en Paternotte over vakantieverhuur van woningen via digitale platforms
3	Motie van de leden Van Ojik en Asscher over het belasten van digitale activiteiten
4	Motie van de leden Asscher en Van Ojik over belastbaarheid van internetgiganten
5	Motie van de leden Alkaya en Moorlag over de onlinemarkt voor aan huis bezorgde maaltijden
	2017 (6 moties)
1	Motie van het lid Pieter Heerma c.s. over de situatie op de markt voor maaltijdbezorging
2	Motie van het lid Nijboer c.s. over digitale diensten betrekken in de belastingheffing
3	Motie van het lid Van der Lee over het gebruik van convenanten in de deeleconomie
4	Motie van het lid Hijink over de juridische status van deeleconomieplatforms
5	Motie van het lid Gijs van Dijk c.s. over de fietskoeriers van Deliveroo
6	Motie van de leden Wiersma en Van Weyenberg over de toekomst van de arbeidsmarkt

Machtsverhoudingen – Eerste Kamer

	2018 (1 motie)
1	Motie-Duthler (VVD) c.s. over digitale transformatie (EK 34.775 VI, V)

Bijlage 2 De betekenis van publieke governance

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 die kunnen helpen 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, oml 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 vorm in een gemeenschappelijke worsteling met politieke problemen en een 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:
1. onderbouwen van het probleem (‘*puzzling’)*;
2. zoeken naar politieke steun (*‘powering*’); en
3. politieke participatie (‘*participation’)*.

In het eerste proces gaat het erom het betreffende probleem goed, bijvoorbeeld met behulp van wetenschappelijk kennis, te onderbouwen 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 moet governance aan een aantal voorwaarden voldoen. Vanuit het besef dat er wereldwijd vele 'falende' of 'fragiele' staten zijn, ontwikkelde 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 governancebegrippen in omloop die verwijzen naar bepaalde typen van interactie tussen de overheid en maatschappelijke actoren

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 governancesysteem

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 governancesysteem.

Het governancevraagstuk gaat dan om de vraag of het governancesysteem, als het geheel aan governance-arrangement rond een bepaald publiek probleem, goed werkt.

Volgens Hoppe (2010) spelen bij het verbeteren van een governancesysteem twee zoekprocessen een rol.

1. 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-risicomaatschappij (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 goverance-ecosysteem waarmee collectieve problemen benoemd en geadresseerd kunnen worden.

2. 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 governancesysteem).

- 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 governancesysteem rond een bepaalde kwestie er uit?

Literatuurlijst bij deze bijlage

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 goverance 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.

© Rathenau Instituut 2018
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.

Open Access
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.

Contactgegevens
Anna van Saksenlaan 51
Postbus 95366
2509 CJ Den Haag
070-342 15 42
info@rathenau.nl
www.rathenau.nl

Bestuur van het Rathenau Instituut
Mw. G. A. Verbeet
Prof. dr. ir. Wiebe Bijker
Prof. mr. dr. Madeleine de Cock Buning
Prof. dr. Roshan Cools
Dr. Hans Dröge
Dhr. Edwin van Huis
Prof. mr. dr. Erwin Muller
Prof. dr. ir. Peter-Paul Verbeek
Prof. dr. Marijk van der Wende
Dr. ir. Melanie Peters - secretaris

Het Rathenau Instituut stimuleert de publieke en politieke meningsvorming over de maatschappelijke aspecten van wetenschap en technologie. We doen onderzoek en organiseren het debat over wetenschap, innovatie en nieuwe technologieën.

Rathenau Instituut