Rathenau Instituut

De stand van digitaal Nederland

Naar zeggenschap en vertrouwen in de digitale samenleving

Rapport

Auteurs
Linda Kool, Jurriën Hamer, Pieter van Boheemen, Romy Dekker, Jasper Deuten, Rinie van Est, Mariëtte van Huijstee, Roos de Jong, Bart Karstens, Eef Masson en Petra Verhoef

Illustraties
Rathenau Instituut

Foto omslag
Drone boven Amsterdam. Travelpixs/Shutterstock

Bij voorkeur citeren als:
Rathenau Instituut (2021). *De stand van digitaal Nederland. Naar zeggenschap en vertrouwen in de digitale samenleving*. Den Haag (auteurs: Kool, L., J. Hamer, P. van Boheemen, R. Dekker, J. Deuten, R. van Est, M. van Huijstee, R. de Jong, B. Karstens, E. Masson, en P. Verhoef)

Voorwoord

Vlak voor het begin van het nieuwe schooljaar 2021/2022 werd onderwijsinstelling ROC Mondriaan in Den Haag gehackt. Bestanden waren onbereikbaar en het computersysteem was platgelegd. Zo'n twee weken later werd bekend dat de criminelen gestolen data, waaronder gegevens over docenten en studenten, online hebben gezet. ROC Mondriaan weigert het 'substantiële bedrag' te betalen dat de criminelen eisen voor het vrijgeven van de gestolen data.

Dergelijke berichten zijn tegenwoordig nauwelijks nog opzienbarend te noemen. Velen zijn zich al langer bewust van de risico's van digitale middelen op het werk en in het dagelijks leven. De afgelopen jaren heeft het Rathenau Instituut uitvoerig onderzoek gedaan naar de digitalisering van de samenleving. Nu is het tijd om de balans op te maken: wat is de stand van digitaal Nederland?

Ons antwoord: de digitale samenleving verkeert in turbulent vaarwater. Datalekken, hacks en de verspreiding van desinformatie zijn aan de orde van de dag. De macht van Big Tech staat een eerlijke economie in de weg. Bedrijven en overheden verzamelen voortdurend data, waarmee ze burgers surveilleren en beïnvloeden. Verspreid over de samenleving zijn ethische codes van kracht, is wetgeving in de maak en zijn afsprakenstelsels opgetuigd. Allemaal nog te vrijblijvend of te zwak om de problemen op te lossen.

Voor dit rapport bundelden we de inzichten uit ons eerdere werk. We selecteerden acht domeinen in de samenleving – van zorg tot onderwijs of openbaar bestuur – en maakten per domein een overzicht van de problemen, onderbelichte vragen in het maatschappelijk debat en de politieke vragen voor de komende vier jaar. Op basis hiervan formuleren we drie speerpunten voor een nieuwe digitaliseringsstrategie: krachtige wetgevingskaders en toezicht, kritisch parlementair debat en zeggenschap voor burgers en professionals over digitale innovatie.

De komende jaren moeten beleidmakers en politici keuzes maken, zodat digitale middelen ons écht een inclusieve democratie, een eerlijke economie, hoogwaardige zorg, onderwijs en bestuur en een duurzame digitale samenleving opleveren. Het Rathenau Instituut ondersteunt de politieke en publieke oordeelsvorming, door onderzoek te doen en de maatschappelijke dialoog te bevorderen.

Drs. Jeroen Heres
Chief scientist, Rathenau Instituut

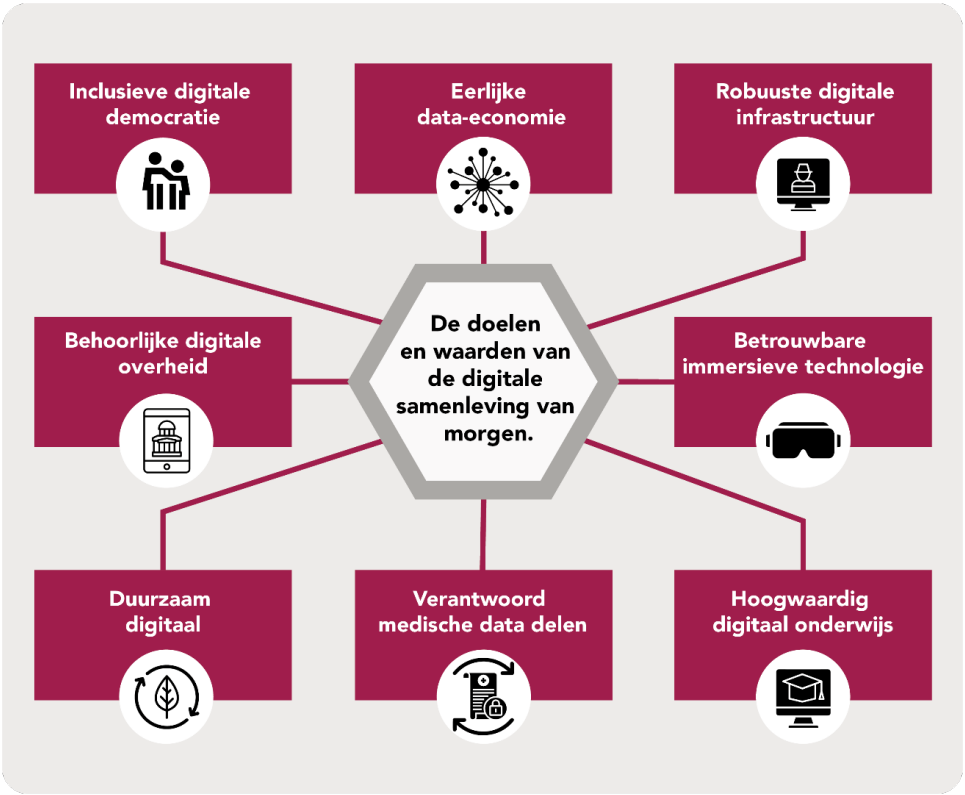
Samenvatting

Turbulent vaarwater voor de digitale samenleving
De afgelopen jaren is de digitale samenleving in turbulent vaarwater terecht gekomen. Het vertrouwen in digitale overheidssystemen liep een grote deuk op door de toeslagenaffaire. De groeiende datahonger van bedrijven, overheden en onszelf heeft geleid tot continue surveillance en beïnvloeding. De macht van Big Tech staat een eerlijke economie in de weg, strekt zich uit tot publieke sectoren en creëert een groeiende afhankelijkheid van buitenlandse techleveranciers voor essentiële diensten als videobellen, email en laptops in de klas. Datalekken, hacks en de verspreiding van desinformatie ondermijnen onze veiligheid en het democratisch debat. En de energierekening van digitale innovaties loopt op, terwijl de samenleving klimaatneutraal moet worden. Prangende kwesties vragen de komende kabinetsperiode om maatschappelijk debat en politieke besluitvorming.

De stand van digitaal Nederland
Dit rapport heeft als doel kabinet en parlement te informeren over de uitdagingen en politieke keuzes die voorliggen. Het Rathenau Instituut bracht de afgelopen jaren publicaties uit over de zorg, het onderwijs, het openbaar bestuur, slimme steden, de nieuwsvoorziening en de energiesector. In dit rapport bundelen we onze inzichten en tonen we de stand van digitaal Nederland in acht domeinen van de samenleving. In deze onderzoeken hanteren we publieke waarden en grond- en mensenrechten als een belangrijk uitgangspunt voor verantwoorde innovatie (Rathenau Instituut 2017a). We beschouwen daarbij grond- en mensenrechten niet slechts als een essentiële ondergrens, maar ook als aansporing tot het realiseren van hoogwaardige maatschappelijke voorzieningen (zie figuur 1).

Dit rapport maakt enerzijds duidelijk dat zich in de samenleving en de politiek allerlei initiatieven ontplooien om publieke waarden bij digitale innovaties te waarborgen. Zo formuleerde het kabinet onder andere de nationale digitaliseringsstrategie, het Strategisch Actieplan AI en de beleidsbrief AI, mensenrechten en publieke waarden. Daarin stimuleert het kabinet onder meer de ontwikkeling van AI-innovaties die voldoen aan ethische richtlijnen en verantwoord datagebruik. Hiervoor zijn ethische codes en hulpmiddelen ontwikkeld. In de zorg- en energiesector zijn afsprakenstelsels voor het delen van data uitgewerkt. Verder onderzocht het kabinet de toekomstbestendigheid van bestaande wettelijke kaders en het bijbehorende toezichtstelsel. In het parlement werd na het rapport van de Tijdelijke Commissie Digitale Zaken de vaste commissie Digitale Zaken opgericht.

Figuur 1 Overzicht van acht urgente vraagstukken voor de digitale samenleving



© Rathenau Instituut

Verlies van zeggenschap en vertrouwen

Maar het blijkt onvoldoende. Dit rapport maakt helder dat de problemen niet zijn opgelost. Onze digitale netwerken zijn nauwelijks veiliger geworden. Wat betreft de bestrijding van desinformatie, zijn vele partijen het eens dat de opgestelde zelfregulering onvoldoende effect heeft. De invloed van Big Tech wordt op steeds meer plekken voelbaar: in de manier waarop we zorg leveren, onderwijs geven, de energiemarkt vormgeven of hoe we zaken in het openbaar bestuur regelen. Het ontbreekt regelmatig aan heldere afspraken die overheden in staat stellen bedrijven ter verantwoording te roepen: bedrijven kunnen voorwaarden en het dienstenaanbod eenzijdig veranderen. De Britse overheid ondervond de gevolgen toen Google en Apple tijdelijk haar Corona-app blokkeerden. Steeds meer scholen en onderwijsinstellingen maken gebruik van de software van Big Tech. Die software bepaalt mede hoe onderwijs vorm krijgt. Deze alsmaar groeiende afhankelijk leidt tot verlies van zeggenschap van burgers, professionals en overheden om digitale innovatie vanuit publieke waarden vorm te geven.

Drie speerpunten voor een nieuwe digitaliseringsstrategie
De samenleving verwacht een inclusieve digitale democratie, een eerlijke data-economie, hoogwaardige digitale middelen voor zorg, onderwijs en bestuur, en een duurzame digitale samenleving. Met het oog op een nieuwe digitaliseringsstrategie, benoemen we daarvoor drie speerpunten:

1. Stel krachtige, toekomstbestendige kaders vast

Het kabinet moet de regie nemen om te zorgen dat digitale innovatie écht bijdraagt aan publieke waarden en grond- en mensenrechten. Dat vraagt om krachtige wettelijke kaders, eisen en randvoorwaarden, met bijbehorend sterk toezicht. De verschillende voorstellen voor nieuwe wettelijke Europese kaders, zoals de Digital Service Act Package en de AI-verordening, bieden hiertoe mogelijkheden. Zij zullen de komende tijd opnieuw vastleggen waar verantwoordelijkheden van bedrijven, overheden, burgers en professionals in de digitale samenleving precies liggen – om daarin keuzes te maken zijn heldere politieke visies nodig. Bovendien is verheldering en aanscherping nodig om de problemen daadwerkelijk aan te pakken. Daarnaast dienen de kaders toekomstbestendig te zijn, en voor te bereiden op de volgende generatie digitale technologie: van 6G tot Virtual Reality, Augmented Reality and spraaktechnologie. Daar is nu nog te weinig aandacht voor.

2. Innoveer waardengedreven, gebaseerd op kritisch parlementair debat

Overheidsbeleid dient gevoed en gecontroleerd te worden door een kritisch parlementair debat over hoe publieke waarden worden gerealiseerd. Publieke waarden zouden in de volle breedte bij het debat betrokken moeten worden, of het nu gaat om digitale leermiddelen in het onderwijs of de geautomatiseerde verzameling van patiëntgegevens. Daarnaast moet de beoogde maatschappelijke opbrengst van digitale innovaties op de parlementaire agenda worden gezet. Deze valt namelijk nog regelmatig tegen. Daarbij is het van belang dat het parlement zelf meer zicht krijgt op digitale systemen bij de overheid, zodat zij nut en noodzaak van digitale innovaties in publieke sectoren periodiek kan toetsten.

3. Creëer zeggenschap voor professionals en burgers

Tenslotte dienen de wettelijke kaders en het gevoerde overheidsbeleid de zeggenschap van professionals en burgers te vergroten. De inzichten van leraren, zorgpersoneel en politieagenten die met digitalisering te maken hebben, moeten worden benut. Hun zeggenschap over digitale innovaties moet worden bevorderd. Daarvoor is het nodig dat overheid en parlement als wetgever de rollen en verantwoordelijkheden van betrokken partijen helder vastleggen. Wat moet bijvoorbeeld een school of ziekenhuis zelf kunnen bepalen? Waar is hulp nodig, en van wie? Waar neemt de overheid regie en hoe dwingt de overheid de naleving van regels en randvoorwaarden af?

Inhoud

Voorwoord 3

Samenvatting 4

Inleiding 9
1.1 Een nieuwe fase voor de digitale samenleving 9
1.2 Doel van dit rapport 10
1.3 Opzet 11

1 Inclusieve digitale democratie 13
1.1 Stand van zaken 13
1.2 Uitdagingen voor beleid en politiek 14
1.3 Welke politieke keuzes liggen voor? 16

2 Eerlijke data-economie 17
2.1 Stand van zaken 17
2.2 Uitdagingen voor beleid en politiek 18
2.3 Welke politieke keuzes liggen voor? 20

3 Robuuste digitale infrastructuur 21
3.1 Stand van zaken 21
3.2 Uitdagingen voor beleid en politiek 22
3.3 Welke politieke keuzes liggen voor? 23

4 Behoorlijke digitale overheid 25
4.1 Stand van zaken 25
4.2 Uitdagingen voor beleid en politiek 26
4.3 Welke politieke keuzes liggen voor? 27

5 Duurzaam digitaal 29
5.1 Stand van zaken 29
5.2 Uitdagingen voor beleid en politiek 29
5.3 Welke politieke keuzes liggen voor? 31

6 Hoogwaardig digitaal onderwijs 33
6.1 Stand van zaken 33
6.2 Uitdagingen voor beleid en politiek 34
6.3 Welke politieke keuzes liggen voor? 35

7 Verantwoord medische data delen 37
7.1 Stand van zaken 37
7.2 Uitdagingen voor beleid en politiek 38
7.3 Welke politieke keuzes liggen voor? 39

8 Betrouwbare immersieve technologie 41
8.1 Stand van zaken 41
8.2 Uitdagingen voor beleid en politiek 42
8.3 Welke politieke keuzes liggen voor? 43

9 Conclusie 45
9.1 De stand van digitaal Nederland 45
9.2 Blinde vlekken in beleid 47
9.3 Naar zeggenschap en vertrouwen 48

Literatuur 52

Inleiding

1.1 Een nieuwe fase voor de digitale samenleving

Leven zonder digitale technologie is voor velen nauwelijks meer voor te stellen. Smartphones, sociale media, slimme camera's en kunstmatige intelligentie – digitale technologie brengt ons in verbinding met anderen, maakt werken op afstand mogelijk, of een gesprek met een docent of dokter. Digitale technologie is onlosmakelijk verbonden met alle onderdelen van onze economie en maatschappij: om tijdig cyberaanvallen te detecteren, vroegtijdig kanker op te sporen of om de balans in een duurzaam energienet te behouden.

Tegelijkertijd is duidelijk dat digitale technologie de samenleving voor grote – en hardnekkige – uitdagingen stelt. Zo bestaan er al jaren grote zorgen over de groeiende stroom datalekken, hacks en gijzelsoftware, en worden onze digitale netwerken er niet of nauwelijks veiliger op. Sociale media, desinformatie en fijnmazige politieke micro-targeting stellen het publieke en democratische debat op de proef. Beleidsmakers buigen zich over de rol en verantwoordelijkheden van de socialemediabedrijven hierin. Het ongemak over de enorme afhankelijkheid van Europa van een handjevol Amerikaanse of Aziatische technologieleveranciers neemt bij velen toe – wie kan nog om de poortwachters heen? Ook op andere terreinen, zoals de digitale systemen van de overheid, de zorg en het onderwijs, zien we hoe digitale technologie diep in kan grijpen op het leven van burgers. Ondertussen stellen klimaatverandering en opkomende technologieën, zoals Virtual en Augmented Reality, spraakherkenning en biometrie, de samenleving voor nieuwe uitdagingen.

Sinds de onthullingen van Edward Snowden en het Cambridge Analytica-schandaal groeide het bewustzijn in de samenleving dat digitalisering publieke waarden onder druk zet (zie ook Rathenau Instituut 2017a; 2018a). Intensieve discussies zijn gevoerd over hoe 'ethische' en 'humane AI' eruit moet zien. Bedrijven, wetenschappers, overheden en internationale instituties als de OESO (2019) en UNESCO (2020) stelden ethische richtlijnen op (zie voor een overzicht Rathenau Instituut 2019g). Die moeten ertoe bijdragen dat kunstmatige intelligentie niet discrimineert en transparante beslissingen neemt.

Ook beleidsmakers en politici erkennen de zorgen en spannen zich in om de uitdagingen te lijf te gaan. Na een periode van zelfregulering en onderzoek naar de mogelijke risico's van digitale technologie, werken overheden overal ter wereld nu

aan de aanscherping van juridische kaders. Zo bereidt de Europese Commissie diverse wetsvoorstellen voor op het vlak van AI, Big Tech, cyberveiligheid en het gebruik van data. Voorbeelden zijn het *Digital Services Act package*, bedoeld om de marktmacht van platformen beter te reguleren en platformen meer verantwoordelijkheden te geven om desinformatie tegen te gaan, de *Data Governance Act,* bedoeld om het delen van data te stimuleren, en het voorstel voor een *verordening over kunstmatige intelligentie*, gericht op het strenger reguleren van AI-toepassingen met een hoog risico op het schenden van mensenrechten.

Het verantwoord vormgeven van de digitale samenleving gaat daarmee een volgende, bepalende fase in. Want de wetten zullen bepalend zijn voor hoe de digitale samenleving er de komende jaren uit gaat zien – op allerlei terreinen zoals gezondheidszorg, energie, onderwijs of economie. Slagen we er in om over vier jaar de samenleving écht veiliger, vrijer, duurzamer en democratischer te hebben gemaakt? Dat zal vragen om politieke keuzes. Want hoewel de maatschappelijke ambities veelal duidelijk zijn, zoals hoogwaardig digitaal onderwijs, verantwoorde medische zorg of een robuuste digitale infrastructuur, is de route daar naartoe minder eenduidig. Tot hoever moeten bijvoorbeeld de verantwoordelijkheden van platformen en overheden precies reiken om desinformatie tegen te gaan? Tot hoever reikt de verantwoordelijkheid van de overheid als het gaat om de toenemende invloed van platformen op het onderwijs?

1.2 Doel van dit rapport

Prangende kwesties vragen de komende kabinetsperiode om maatschappelijk debat en politieke besluitvorming. Cruciaal is de oprichting van de vaste commissie Digitale Zaken in de Tweede Kamer, in navolging van de conclusies van de tijdelijke commissie Digitale Toekomst. Het Rathenau Instituut was nauw betrokken in de fase voorafgaand aan de oprichting van de vaste commissie Digitale Zaken; op verzoek van de tijdelijke commissie Digitale Toekomst schreven we het rapport ‘Meer grip op digitalisering’, waarin we in kaart brachten hoe parlementen in andere landen zichzelf organiseren rondom digitalisering (Rathenau Instituut 2020a).

Ook een volgend kabinet zal zich buigen over digitalisering en naar verwachting een nieuwe digitaliseringsstrategie. Het doel van dit rapport is om de commissie Digitale Zaken en het nieuwe kabinet te informeren over de uitdagingen, beleidsopties en politieke keuzes die de komende jaren voorliggen. In een bijbehorend Bericht aan het parlement richten we ons specifiek tot de commissie Digitale Zaken (Rathenau Instituut 2021f).

1.3 Opzet

Het Rathenau Instituut deed de afgelopen jaren onderzoek en voerde gesprekken met vele stakeholders over hoe publieke waarden digitale innovaties in diverse domeinen, zoals het openbaar bestuur, de zorg, energie en het onderwijs, worden gerealiseerd. Verder deden we onderzoek naar, en zwengelden we het debat aan over, nieuwe digitale technologie, zoals kunstmatige intelligentie en immersieve technologie – technologie die je steeds verder onderdompelt en meesleept in de digitale wereld, zoals Virtual Reality, Augmented Reality en spraaktechnologie. Ook onderzochten we innovatieprocessen en het innovatiebeleid in Nederland en Europa. In al deze onderzoeken hanteren we grond- en mensenrechten als belangrijk uitgangspunt, waarbij we deze rechten niet slechts beschouwen als essentiële ondergrens, maar als aansporing tot het realiseren van hoogwaardige maatschappelijke voorzieningen.

Dit rapport bundelt onze inzichten van de afgelopen jaren uit acht domeinen. In de volgende acht hoofdstukken lichten we ieder domein nader toe. Per domein geven we aan welke maatschappelijke en ethische kwesties op de beleidsagenda zijn gekomen voor welke kwesties nog weinig aandacht is, en welke beleidsopties en politieke keuzen voorliggen om digitalisering verantwoord vorm te geven. Onderstaande tabel vat per domein de belangrijkste politieke vraagstukken samen.

Tabel 1 Samenvatting politieke vraagstukken van de digitale samenleving

Domein	Vraagstukken
Inclusieve digitale democratie	Desinformatie, deepfakes, politieke micro-targeting en de macht van Big Tech bedreigen de democratie. In Europese wetsvoorstellen krijgen platformen meer verantwoordelijkheden. Maar hoe ver moeten die precies reiken? Is het toezicht voldoende geregeld als platformen gaan bepalen wat illegale content is? Digitale middelen kunnen democratische besluitvorming ook versterken. In welke mate willen partijen daar gebruik van maken?
Eerlijke data-economie	Platformen brengen vraag en aanbod efficiënt bij elkaar, maar de enorme marktmacht onzekere arbeidsomstandigheden en minder leefbare steden zijn bekende keerzijden. Nieuwe wetten moeten de marktmacht reguleren en investeringen in Europese technologie moet zorgen voor alternatieve aanbieders. Maar met meer concurrentie ontstaat nog geen leefbare stad. Welke plichten moeten platformen krijgen om een eerlijke economie te realiseren? En hoe kan innovatiebeleid meer worden gericht op maatschappelijke uitdagingen?

Robuuste digitale infrastructuur	De digitale samenleving is kwetsbaar. Hoewel de afgelopen jaren meer wettelijke eisen zijn opgesteld, bijvoorbeeld voor 5G, blijft de basis, zoals encryptie, onvoldoende op orde. De afhankelijkheden worden groter. En nieuwe infrastructuren, zoals 6G en satellieten, komen eraan. Wat is er nodig om Nederland veiliger te maken en hoeveel mag dat kosten? Hoe kan Nederland haar hoogwaardige expertise over kwantumtechnologie, encryptie en AI beter benutten?
Behoorlijke digitale overheid	De overheid gebruikt data en algoritmen om te beslissen over zaken die burgers aangaan. Maar die beslissingen zijn vaak ondoorzichtig. En het blijkt lastig om maatwerk te leveren en gemaakte fouten snel te herstellen. Bovendien blijken systemen niet altijd effectief. Hoe weegt het parlement de maatschappelijke kosten tegen de baten? Wat is er nodig om te waarborgen dat digitale overheidssystemen voldoen aan de eisen van behoorlijk bestuur?
Duurzaam digitaal	Digitalisering van het energiesysteem kan de energietransitie bevorderen. Dat vraagt om beter gebruik van energiedata, met aandacht voor privacy en beveiliging. Dat is nog niet voor alle relevante data, zoals data uit slimme thermostaten of elektrische auto's, goed geregeld. Hoe zorgt het parlement dat beschikbare data in dienst staat van de energietransitie? En hoe wordt gezorgd dat de ambities voor digitalisering gelijk op gaan met de doelen van de energietransitie?
Hoogwaardig digitaal onderwijs	Onderwijsinstellingen experimenteren met digitale leermiddelen. Op beleidsniveau is aandacht voor dataprotectie, beveiliging en publieke regie over de inkoop van systemen. Maar de impact van educatieve technologie reikt verder dan dat. Want wat betekenen de systemen voor de kwaliteit van het onderwijs en kansengelijkheid? Durven leerlingen nog fouten te maken als elke stap wordt vastgelegd? Kortom: hoe kan innovatie vorm worden gegeven met oog voor onderwijskwaliteit en publieke waarden?
Verantwoord medische data delen	Uitwisseling van medische data kunnen de gezondheidszorg vooruit helpen, bijvoorbeeld doordat zorgverleners over de juiste informatie beschikken. Maar het gebruik van medische data dient uiterst zorgvuldig, en in het belang van de publieke gezondheidszorg, te gebeuren. Met de toename van private partijen en grote platformen komt dat belang onder druk te staan. Hoe behouden we solidariteit bij datagebruik en worden zorgverleners en patiënten beter beschermd?
Betrouwbare immersieve technologie	Spraaktechnologie, Virtual Reality en Augmented Reality maken het nog moeilijker om echt van nep (manipulatie) te onderscheiden. Deze technologieën zullen de komende jaren worden gebruikt in de zorg, het onderwijs, de bouw of defensie. Welke afspraken zijn er nodig over privacy, autonomie, waarachtigheid en gezondheid? En welke juridische kaders ontbreken, zoals voor onze publieke ruimte en intellectueel eigendom?

1 Inclusieve digitale democratie

1.1 Stand van zaken

Digitalisering transformeert onze democratie. Bestaande democratische processen, zoals het publieke debat, de verkiezingen en parlementaire representatie, deliberatie en besluitvorming, veranderen en staan steeds vaker onder druk. Het verspreiden van desinformatie en deepfakes kan bijvoorbeeld maatschappelijke tegenstellingen aanwakkeren en wantrouwen in politieke instituties voeden. Politieke microtargeting, het gericht verzenden van politieke advertenties naar bepaalde doelgroepen, kan een kiezer op een ondoorzichtige manier beïnvloeden en leiden tot een versplintering van het publieke debat. Het online publieke debat blijkt kwetsbaar te zijn voor manipulatie (Rathenau Instituut, 2020b).

Digitalisering biedt tegelijkertijd nieuwe mogelijkheden voor interactie tussen burgers, politici en bestuurders. Maar digitale platformen en gadgets maken nog geen digitale democratie (Rathenau Instituut, 2017b). In het verleden leidden ervaringen met digitale burgerparticipatie bijvoorbeeld vaak tot teleurstelling bij deelnemers. Digitale instrumenten hebben wel de potentie om bij te dragen aan gebalanceerde informatie- en communicatiestromen, waardoor parlement, regering, burgers, stakeholders en media elkaar kunnen voeden en corrigeren. Veel van de populaire socialemediaplatformen zijn hier echter niet voor ontworpen en bereiken soms eerder het tegendeel.

De zorgen over het polariserende effect van algoritmen op de platformen en de vatbaarheid van het publieke debat voor desinformatie en ongewenste buitenlandse beïnvloeding, staan inmiddels hoog op de beleidsagenda. Het kabinet werkte al aan scherpere randvoorwaarden en waarborgen om de impact van digitalisering op het publieke debat te reguleren. Zo loopt het traject om de Wet op politieke partijen te herzien, met daarin aandacht voor manipulatieve digitale technieken zoals microtargeting. Ook worden de Europese richtlijnen op het gebied van desinformatie (*EU Action Plan on Disinformation*) uitgewerkt.

De Europese Commissie bereidt strengere regelgeving voor over de macht en verantwoordelijkheden van platformen voor de verspreiding van desinformatie en illegale content (*Digital Services Act* en *Digital Markets Act*). Het in december gelanceerde *European Democracy Action Plan* is specifiek gericht op maatregelen om eerlijke en vrije verkiezingen te waarborgen, mediavrijheid te versterken en

desinsformatie tegen te gaan. Dit plan vervangt het hier bovengenoemde, meer vrijblijvende, actieplan over desinformatie.

Tot slot werken beleidsmakers aan versterking en vernieuwing van democratie (programma Democratie in Actie; Kamerstukken 34775-VII nr. 69; Kamerstukken 2020Z12861). De staatscommissie parlementair stelsel (commissie Remkes) wijst op onvolkomenheden in de inhoudelijke vertegenwoordiging in het Nederlandse parlement, en uit periodieke enquêtes van het SCP blijkt dat burgers méér willen meebeslissen over belangrijke politieke kwesties (staatscommissie parlementair stelsel, 2018).

Op lokaal niveau gebeurt dat al. Gemeenten experimenteren met alternatieve vormen van digitale burgerbetrokkenheid (Rathenau Instituut, 2019a). Op nationaal niveau blijft burgerbetrokkenheid nog achter, ondanks nieuwe ambities, zoals een nieuwe vorm van jongereninspraak op landelijk niveau (Kamerstukken 2020Z12861). Ook in het buitenland is inspiratie op te doen, bijvoorbeeld op het gebied van interactieve online consultaties, het visualiseren van het meningenlandschap en digitaal co-creëren of steunen van voorstellen of initiatieven (Rathenau Instituut, 2020c).

1.2 Uitdagingen voor beleid en politiek

Beleidsmakers richtten zich de afgelopen periode op twee zaken: enerzijds te proberen de negatieve impact van platformen te begrenzen en anderzijds te experimenteren met instrumenten voor digitale burgerbetrokkenheid. De begrenzing van de negatieve impact van platformen krijgt met name vorm door aangescherpte wettelijke kaders op het vlak van politieke advertenties, profilering, transparantieverplichtingen voor socialemediaplatformen.Ook de begrenzing van marktmacht speelt een rol, zie Hoofdstuk 2 Eerlijke data-economie. Een grote politieke vraag is: hoe ver reikt de verantwoordelijkheid van platformen precies? Veel partijen zien ook het risico van censuur: dat socialemediaplatformen bepalen wat er wel of niet gezegd mag worden in het publieke en politieke debat.

De experimenten met het versterken van burgerbetrokkenheid draaien al snel om het creëren en goed functioneren van nieuwe online tools. Maar voor vruchtbare, vrije en veilige interactie tussen burgers, politici en bestuurders is meer nodig dan technologie. Welke verwachtingen worden bij burgers gewekt over hun inbreng? In hoeverre willen bestuurders en politici de aangedragen ideeën realiseren? Politieke wil om de uitkomsten van burgerbetrokkenheid mee te wegen, en het managen van de verwachtingen bij burgers over hoe hun inbreng meeweegt in het besluitvormingsproces, zijn dus cruciale succesfactoren. Daarnaast blijkt het ook

online lastig om nieuwe en diverse groepen te bereiken. Nieuwe participatiemogelijkheden worden met name benut door welgestelde, hoogopgeleide mannen van middelbare leeftijd (Van der Meer, 2018; Hurenkamp en Tonkens, 2019). Met nieuwe kanalen worden dus vaak dezelfde politiek actieve burgers bediend en wordt de ongelijkheid juist groter.

Ook is er te weinig aandacht voor de benodigde digitale vaardigheden voor online participatie in democratische processen. Zonder te investeren in technologisch burgerschap dreigen niet-politiek-actieve burgers nog verder onder de radar verdwijnen.

Volksvertegenwoordigers laten hier zelf ook kansen liggen; digitale instrumenten kunnen meer worden benut voor de controlerende, agenderende en wetgevende taken van het parlement. Gemodereerde platformen voor interactie – van korte consultaties tot uitgebreide deliberaties – en systemen die informatie vind- en doorzoekbaar maken, kunnen de verbinding tussen burger, politiek en de overheid versterken, en de transparantie van het politieke proces vergroten. Dit vergt wel debat over wat de gewenste plek en rol van digitale democratische instrumenten. In een representatieve democratie bestaat er immers een spanning tussen meer burgerbetrokkenheid en de autonomie van het parlement om belangen en waarden tegen elkaar af te wegen.

Figuur 2 Overzicht van kwesties en politieke vragen voor een inclusieve digitale democratie

© Rathenau Instituut

1.3 Welke politieke keuzes liggen voor?

- Bedreigingen van het politieke debat adresseren: tot hoever moeten de verantwoordelijkheden van platformen reiken? Om de nadelige gevolgen daadwerkelijk aan te pakken, zullen de voorliggende wetsvoorstellen verder moeten worden aangescherpt. Bijvoorbeeld ten aanzien van de verspreiding van schadelijke content, gepersonaliseerde advertenties, transparantie of risico op censuur, of tten aanzien van politieke micro-targeting van burgers. Lees meer in de berichten: 'De toekomst van online platformen' (Rathenau Instituut, 2021a) en 'Desinformatie bestrijden, censuur vermijden' (Rathenau Instituut 2020d).

- Burgerbetrokkenheid stimuleren: in welke mate dient er gebruik te worden gemaakt van digitale middelen om burgerbetrokkenheid te vergroten? Welke middelen zijn wenselijk in welk proces, of fase van de beleidscyclus? Het gebruik van digitale middelen in de democratie vergt experiment, reflectie en herhaling. Alleen dan kan digitale burgerparticipatie bijdragen aan democratische legitimiteit. Een leerproces faciliteren is dus essentieel – vind niet telkens het wiel opnieuw uit. Onderzoek naar de langetermijneffecten van digitale burgerbetrokkenheid op het vertrouwen tussen burgers en politiek en de overheid zijn cruciaal om te kunnen leren en verbeteren. Lees meer in het bericht 'Met digitale middelen besluitvorming verbeteren' (Rathenau Instituut 2020e).
- Digitale innovatie voor het parlement: in hoeverre dient het parlement zelf gebruik te maken van digitale middelen om haar processen en taak te verbeteren? Welke mate van transparantie en verbetering van kwaliteit van besluitvormingsprocessen is nodig? En in welke mate is het wenselijk de middelen in te zetten om beleid te evalueren en bij te stellen? Het parlement kan hiertoe een digitale innovatieagenda opstellen, om de kansen van nieuwe technologie te benutten. Zie ook 'Met digitale middelen besluitvorming verbeteren' (Rathenau Instituut 2020e).

- Houd bepaalde processen niet digitaal: Sommige democratische processen zijn zo essentieel, bijvoorbeeld voor inclusie, menselijk contact en cybersecurity, dat analoge alternatieven nodig zijn en blijven – zoals stemmen tijdens verkiezingen. Het is van belang om waakzaam te zijn voor veiligheidsrisico's en uitsluiting van groepen burgers, bijvoorbeeld door gebrek aan digitale vaardigheden of vatbaarheid voor manipulatie. Zie ook ons rapport 'Cyberweerbaar met nieuwe technologie' (Rathenau Instituut 2020f).

2 Eerlijke data-economie

2.1 Stand van zaken

Lange tijd werden vooral de voordelen van online platformen voor consument en maatschappij gevierd: de innovaties maakten het makkelijk om spullen te delen, om vraag en aanbod efficiënt en zonder tussenpersonen samen te brengen en ze verbonden ons met vrienden en familie over de hele wereld. Maar inmiddels zijn de nadelen van online platformen ook zichtbaar: het effect van Airbnb op de hotelbranche en leefbaarheid in steden, het effect van bol.com op de winkelstraten, van Uber op de arbeidsomstandigheden van taxichauffeurs en het effect van de ondoorgrondelijke algoritmen van Facebook, Youtube en Twitter op het publieke debat (Rathenau Instituut 2017c).

De groeiende macht van de Big Tech platformen, waaronder Google, Apple, Facebook, Amazon en Microsoft (GAFAM), alsook Chinese bedrijven als Tencent en Alibaba, is beleidsmakers een doorn in het oog. De dominantie van deze partijen uit zich niet alleen in marktmacht, maar ook in datamacht. De platformen verzamelen enorme hoeveelheden data, die gebruikt worden om burgers te profileren, bepaalde informatie te tonen en advertenties en prijzen ‘op maat’ aan te bieden. De platformen breiden hun dienstverlening steeds verder uit: bijvoorbeeld van zoekmachine, mailserver, browser en besturingssysteem, tot onderwijstool of gezondheidshulp. De databerg van de platformen wordt steeds groter en wordt gebruikt om software te trainen en nieuwe diensten te lanceren. Dat zet nieuwkomers op achterstand. Bovendien leveren de grote platformen in toenemende mate de infrastructuur voor het online publieke debat, dat met de verspreiding van desinformatie, de opkomst van deepfakes en politieke microtargeting ook onder druk staat (zie ook hoofdstuk 1: Inclusieve digitale democratie).

De grote gemene deler in deze verscheidenheid aan problemen, is dat de zeggenschap en positie van burgers, consumenten, werknemers en MKB ten opzichte van de grote online platformen uit balans is geraakt. Beleidsmakers en politici zoeken naar manieren om die balans te herstellen. Zo is de ambitie van een ‘concurrerende, eerlijke en transparante digitale economie’ een van de pijlers in de Nationale Digitaliseringsstrategie (Ministerie van Economische Zaken en Klimaat, 2018). Het kabinet heeft onder andere geïnvesteerd in expertise bij de toezichthouder Autoriteit Consument en Markt (ACM) en onderzoekt manieren om het mededingingsbeleid aan te scherpen. Verder heeft het kabinet zelfregulering in

diverse sectoren aangemoedigd, zoals restaurants of de huizenmarkt, om te stimuleren dat particuliere aanbieders ook kunnen toetreden tot de digitale markt.

Ook de Europese Commissie heeft de afgelopen jaren een breed pakket aan wetsvoorstellen gelanceerd. Het consumentenrecht is vernieuwd, kleine aanbieders zijn beter beschermd tegen handelsplatformen (EU-verordening 2019/1150) en in december 2020 presenteerde de Commissie het *Digital Services Act*-pakket (Europese Commissie, 2020). De *Digital Market Act* (wet inzake digitale markten) is het economische deel van het pakket en gericht op de grote poortwachters. Het wetsvoorstel creëert meer mogelijkheden om platformen voorafgaand aan de implementatie van toepassingen te reguleren. De *Digital Service Act* (wet inzake digitale diensten) is het maatschappelijke deel van het pakket en gericht op strengere verantwoordelijkheden van platformen, o.a. op het gebied van desinformatie en politieke microtargeting (Rathenau Instituut 2020b).

Naast strengere regulering richt de Europese Commissie zich op de ontwikkeling van Europese technologie, onder de noemer ‘technologische soevereiniteit’ (Von der Leyen, 2019). De wens groeit om minder afhankelijk te worden van buitenlandse technologieleveranciers. En dus wil de Europese Commissie dat Europa koploper wordt in o.a. kunstmatige intelligentie, quantum computing, robotica en cloud computing. Dat wil de Commissie doen via missiegedreven innovatiebeleid, dat ook steeds meer een Nederlandse beleidsaanpak is.

2.2 Uitdagingen voor beleid en politiek

De grote uitdaging is *hoe* dat beleid vorm te geven in de praktijk. Het missiegedreven innovatiebeleid is een trendbreuk met de afgelopen decennia. Voorheen was innovatiebeleid vooral gericht op het stimuleren van meer R&D-investeringen door bedrijven. In maatschappelijke missies is economische groei niet langer het primaire doel – het draait om onderzoek en innovatie actiever te richten op het aanpakken van complexe maatschappelijke vraagstukken. Niet de technologische belofte staat centraal, maar de behoefte bij burgers en praktijkorganisaties om maatschappelijke veranderingen in gang te zetten of te versnellen. Het vertrekpunt van het innovatiebeleid is het wegnemen van knelpunten voor systeemveranderingen, bijvoorbeeld in de energiesector. Hiervoor zijn allerlei vernieuwingen nodig – niet alleen op technologisch vlak, maar ook met betrekking tot verdienmodellen, productieprocessen, regulering, standaarden, protocollen, routines of opvattingen van gebruikers of burgers. Om dit nieuwe genre innovatiebeleid te onderscheiden van het technologie- en bedrijvengerichte innovatiebeleid, spreken we van opgavegericht innovatiebeleid (Rathenau Instituut 2020g).

Maar uit onderzoek van het Rathenau Instituut blijkt dat opgavegericht innovatiebeleid in de praktijk nog in de kinderschoenen staat. Het innovatiebeleid blijft vooral gericht op technologieontwikkeling en op het verdienvermogen van bedrijven – bijvoorbeeld in de Groeibrief (Rathenau Instituut 2021c). In haar *Whitepaper on AI* noemt de Commissie terreinen waarop AI kan bijdragen aan maatschappelijke uitdagingen, zonder te preciseren wat de uitdagingen zijn (Rathenau Instituut 2020h). Ook kijken Europa en Nederland vooral naar publiek-private-samenwerking om maatschappelijke uitdagingen te realiseren. Succesvolle inbedding van innovaties vergt echter nauwe samenwerking tussen veel meer partijen, bijvoorbeeld tussen regelgevende instanties, professionals op de werkvloer, vertegenwoordigers van het maatschappelijk middenveld en burgers. De Europese Commissie en Nederland zullen dus meer moeten doen dan alleen investeren in nieuwe technologie. Burgers, praktijkprofessionals, uitvoeringsorganisaties in de publieke sector en maatschappelijke organisaties moeten medezeggenschap krijgen over de kennis- en innovatieagenda's van het opgavegerichte innovatiebeleid.

Het verbreden van de blik heeft ook betrekking op regulering. Regulering is een belangrijk onderdeel van de maatschappelijke inbedding van innovaties. De aandacht lijkt voorlopig vooral gericht op de regulering van platformen: meer concurrentie en meer transparantie creëren bij de grote platformen. Maar meer transparantie en concurrentie alleen lossen nog niet de problemen op waar we dit stuk mee begonnen: meerdere Ubers leveren niet automatisch een eerlijke taximarkt op waarin chauffeurs een eerlijk loon verdienen; meerdere Airbnbs resulteren niet automatisch in leefbare steden; en meerdere Facebooks garanderen nog geen transparant publiek debat. Daarom is het van belang dat Nederland en Europa een brede blik houden met betrekking tot publieke waarden en maatschappelijke uitdagingen.

Figuur 3 Overzicht van kwesties en politieke vragen voor een eerlijke data-economie

© Rathenau Instituut

2.3 Welke politieke keuzes liggen voor?

- Regulering van platformen: hoe kan bij voorliggende wetsvoorstellen (*Digital Service Act Package*) meer rekening gehouden worden met de cruciale rol die platformen in de digitale infrastructuur hebben gekregen? Hoe dienen verantwoordelijkheden behorend bij die nutsfunctie te worden belegd? Is er meer publieke regie nodig om semipublieke sectoren zoals onderwijs, gezondheid en de energiesector vorm te geven vanuit publieke waarden? Lees voor meer informatie onze berichten 'De toekomst van online platformen' (Rathenau, 2021a) en 'Online platformen, offline impact' (Rathenau Instituut 2020i).

  Reikwijdte van het innovatiebeleid bepalen: welke mate van regie, en welke beleidsinstrumenten, zijn nodig om het innovatiebeleid vanuit maatschappelijke uitdagingen en publieke waarden vorm te geven? Welke kennis, welke innovatieve activiteiten en welke partijen zijn nodig? En hoe ver dient de politiek vooruit te kijken om maatschappelijke uitdagingen effectief te adresseren? Dit vraagt om een nieuw genre opgavegericht innovatiebeleid, waarin een passend instrumentarium en investeringsbudget is uitgewerkt, en eisen worden gesteld aan organisaties en personen die innovatieprogramma's aansturen. Lees meer in het bericht 'Maak werk van opgavegericht innovatiebeleid' (Rathenau Instituut 2020j).

3 Robuuste digitale infrastructuur

3.1 Stand van zaken

De digitale samenleving is een kwetsbare samenleving (Rathenau Instituut 2017d; Rathenau Instituut 2020f). Met de voortschrijdende digitalisering van de samenleving worden steeds meer gegevens digitaal verwerkt, gebruiken we steeds meer digitale apparaten en diensten en worden we steeds afhankelijker van deze diensten. Al deze data, apparaten en diensten kunnen uitvallen, worden gehackt, of worden gebruikt voor spionage. Steeds weer blijkt dat de beveiliging van apparaten en diensten niet op orde is. Soms door menselijke fouten of gebrek basismaatregelen, zo lieten de datalekken in de GGD-systemen zien.

Maar ook organisaties die zwaar toegerust zijn om de digitale beveiliging op orde te hebben, lukt dit niet altijd. En steeds vaker worden deze zwakheden benut door kwaadwillenden om te infiltreren in netwerken, informatie te stelen of te saboteren. Er is sprake van een oplopend informatieconflict (Rathenau Instituut 2019b). Eind 2020 kwam bijvoorbeeld de SolarWinds hack aan het licht. Daarmee heeft een Russische groepering zeer waarschijnlijk toegang weten te verkrijgen tot de IT-systemen van duizenden organisaties, waaronder die van het Europees Parlement, NAVO, diverse Amerikaanse overheidsorganisaties en die van techgiganten als Microsoft.

Een bijkomend probleem is de groeiende afhankelijkheid van organisaties en gebruikers van de technologie van buitenlandse technologiebedrijven, veelal uit de VS en China. Onder andere het toenemend gebruik van clouddiensten vergroot de risico’s op uitval bij verstoring en verlies van controle en zeggenschap over data en dataverwerking (Rathenau Instituut 2020f). Hierbij zien Nederland en Europa zich geconfronteerd met volatiele internationale omstandigheden. Er ontstond een politieke machtsstrijd tussen de Verenigde Staten en China, waarbij deze landen elkaar beschuldigden van spionage en inmenging. Deze spanningen spitsten zich met name toe op een mogelijk verband tussen 5G-leveranciers en landen met een offensief cyberprogramma gericht op Nederland of Europa. Met name rondom de apparatuur van Huawei is veel discussie ontstaan.

In de afgelopen jaren is er bij beleidsmakers in Nederland en Europa steeds meer aandacht gekomen voor het cyberweerbaar maken van de samenleving. Zo stelt de Wet beveiliging netwerken- en informatiesystemen (Wbni) strengere eisen aan aanbieders van diensten en infrastructuur, wordt er gewerkt aan strengere eisen voor Internet of Things apparatuur via een update van de *Radio Equipment Directive*, zijn er expertisecentra opgericht om meer te delen (Staatssecretaris

Keijzer, 2020) en zijn er programma's gericht op het ontwikkelen van kennis, expertise en bewustzijn. In 2020 werd bijvoorbeeld het Samenwerkingsplatform 'Cybersecurity kennis en innovatie' (Dcypher) opgericht.

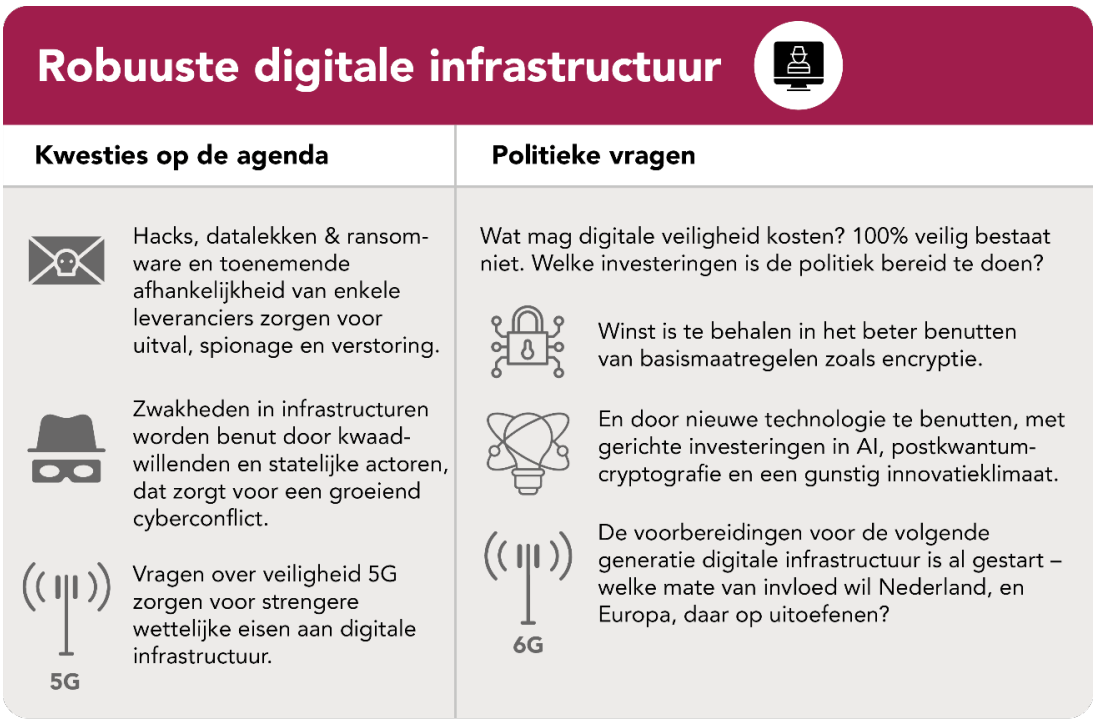
3.2 Uitdagingen voor beleid en politiek

Al deze inspanningen ten spijt, luiden instanties als de Algemene Rekenkamer (2019a, 2019b), de WRR (2019), de NCTV (NCBN 2020; 2021), de Cyber Security Raad (2021a; 2021b) en het Rathenau Instituut (2017d, 2020f) onverminderd de noodklok over de situatie in Nederland. Maatschappelijke ontwrichting ligt op de loer, onze (bedrijfs)geheimen liggen op straat of worden gestolen. Nederland bereidt zich te weinig voor op situaties van daadwerkelijke uitval van systemen. Het is lastig om effectief te handhaven en actief invulling te geven aan open normen. Bovendien suggereert Nederland omwille van opsporing te willen tornen aan de integriteit van een van de weinige instrumenten om digitale veiligheid mee te creëren: encryptie (Hamer en Kool 2021).

Bovendien tekent zich in Europa en Nederland een groeiend ongemak af over de afhankelijkheid van buitenlandse techbedrijven. Bij het aantreden van de nieuwe Europese Commissie lanceerde Ursula von der Leyen daarom het idee van 'technologische soevereiniteit', waarmee zij wijst op het belang van het toewijzen van verantwoordelijkheden, het afleggen van verantwoordelijkheid en praktische veiligheidsstandaarden (Von der Leyen 2019). De afhankelijkheid kan niet alleen leiden tot uitval van essentiële diensten en kritieke infrastructuur, en daarmee ontwrichting van economie en maatschappij, maar leidt ook tot verminderde zeggenschap van overheid en professionals over publieke sectoren (zie hoofdstuk 6: Hoogwaardig digitaal onderwijs en hoofdstuk 7: Verantwoord medische data delen), en kan democratische processen schaden (zie hoofdstuk 1: Inclusieve digitale democratie, en CSR 2021b).

Tot nu verwachten Nederland en Europa dat vooral de ontwikkeling van nieuwe technologie hen zal helpen om minder afhankelijk te worden van buitenlandse technologieleveranciers. In Nederland is op specifieke gebieden als kwantumtechnologie, encryptie en kunstmatige intelligentie unieke kennis aanwezig. Met deze kennis kunnen veiligere producten en diensten worden ontwikkeld. Daar is grote behoefte aan. De aanwezige kennis geeft Nederland en Europa de mogelijkheid om hun eigen IT-bedrijvigheid te stimuleren. Om die veiligere en soms duurdere producten een kans te geven, is een stimulerend beleid nodig. Dit rapport laat zien dat ook op andere terreinen nadere afspraken nodig zijn om zeggenschap te behouden over publieke sectoren, openbaar bestuur en democratische processen.

Figuur 4 Overzicht van kwesties en politieke vragen over een robuuste digitale infrastructuur



© Rathenau Instituut

3.3 Welke politieke keuzes liggen voor?

- Benut basismaatregelen beter: Investeringen in het cyberweerbaar maken van Nederland kosten geld. En 100% veilig bestaat niet. Welke risico's moeten zoveel mogelijk worden uitgesloten, en welk prijskaartje zijn partijen bereid daarvoor te accepteren? Winst is te behalen door het beter benutten van basismaatregelen, zoals sterke encryptie en open data standaarden, en door strengere eisen aan vitale infrastructuur, diensten en aanbieders. In het energiedomein (zie hoofdstuk vijf: Duurzaam digitaal) geven we aan dat er nog te weinig geregeld is voor energiedata afkomstig van apparaten van commerciële partijen. Lees meer in ons rapport Cyberweerbaar met nieuwe technologie (Rathenau Instituut 2020f).
- Benut de kansen van nieuwe technologie: Kennis over een aantal veiligheidstechnieken (kwantumencryptie en kunstmatige intelligentie) is in Nederland op wereldniveau en kan beter worden benut. De overheid kan daarbij ook zelf het voortouw nemen, door als launching-customer op te treden of bij inkoopvoorwaarden meer eisen te stellen aan veiligheid. Dat vraagt een daadkrachtiger kennis- en innovatiebeleid, met meer focus in de

onderwerpen van de Nederlandse Cyber Security Research Agenda (NCSRA). Ook een gunstig innovatieklimaat, met aantrekkelijkere aanbestedingsprocedures voor innovatieve startups is daarbij van belang. Zo kan Nederland investeren in strategische digitale autonomie. Zie het rapport Cyberweerbaar met nieuwe technologie (Rathenau Instituut 2020f).

- Investeren in de volgende generatie digitale infrastructuur: De huidige politieke debatten draaien om de uitrol van 5G, maar de ontwikkeling van de volgende generatie digitale infrastructuur krijgt al vorm, zoals 6G en satellieten. Welke financiële en beleidsmatige investeringen is Nederland bereid te doen, zodat de samenleving kan profiteren van deze nieuwe technologieën? Hoe wil Nederland invloed uitoefenen in internationale fora, zodat bij de ontwikkeling van protocollen en standaarden aandacht is voor veiligheid en gezondheidsrisico's? Lees meer in het bericht '5G-debat behoeft meer diepgang' (Rathenau Instituut 2020k).

4 Behoorlijke digitale overheid

4.1 Stand van zaken

De overheid digitaliseert in hoog tempo en dat heeft gevolgen voor de rechtsstaat. De afgelopen jaren is gebleken dat geautomatiseerde overheidsbesluitvorming tal van risico's oplevert voor de bescherming van grondrechten en voor het respecteren van de principes van behoorlijk bestuur (Rathenau Instituut, 2021c; ROB 2021). Zo blijken op algoritmes gebaseerde overheidsbesluiten soms onvoldoende uitlegbaar en kan het erg moeilijk zijn om fouten te herstellen en maatwerk te leveren. Bij het koppelen van data en (risico-)profilering staan tevens privacy-, vrijheid- en gelijkheidsrechten onder druk. Voor het parlement is het steeds lastiger om te controleren of de uitvoerende macht handelt binnen de grenzen van de wet (Passchier, 2021). En op haar beurt is het voor de regering steeds lastiger om technologiebedrijven waarmee zij samenwerkt, met name Big Tech, doortastend te reguleren. De keuzes die vroeg in het ontwerpproces worden gemaakt en de werkelijke impact van systemen op individuele levens, blijven geregeld onzichtbaar. Het ontbreekt op verschillende niveaus aan effectieve tegenmacht.

Met de toeslagenaffaire zijn veel van de risico's bewaarheid. De overheid schond op grote schaal de rechten van burgers en bleek jarenlang niet in staat – of niet ter wille – om het onrecht effectief aan te pakken. Ook het Systeem Risico Indicatie (SyRI) bleek geen verbetering op te leveren in de fraudeopsporing, was onvoldoende controleerbaar en schond privacyrechten, zo oordeelde de rechter uiteindelijk. Toch hebben deze affaires het enthousiasme voor de digitale overheid en voor geavanceerde AI-systemen niet doen afnemen. Het wetsvoorstel 'Gegevensverwerking door Samenwerkingsverbanden' (ook wel Super SyRI genoemd) is in de Tweede Kamer aangenomen en ligt nu voor in de Eerste Kamer. Met name uitvoeringsorganisaties experimenteren bovendien volop met AI-innovaties (TNO, 2019; ARK, 2021). Bij tal van taken, zoals het toekennen van toeslagen, het verlenen van vergunningen, of het innen van verkeersboetes, kunnen zij eigenlijk ook niet meer zonder AI-innovaties en liggen kansen om overheidsdiensten en hulpverlening met deze innovaties goedkoper én beter te maken.

Wel staan mede vanwege genoemde misstanden de rechtsstatelijke kwesties rondom een digitaliserende overheid op de beleidsagenda. Het kabinet constateert dat de bestaande wettelijke kaders, waaronder de Grondwet, de Algemene wet

bestuursrecht (Awb) en de Algemene Verordening Gegevensbescherming (AVG), voldoende mogelijkheden bieden om softwaresystemen te reguleren. Voor het dichten van een aantal lacunes wacht het kabinet op nadere wettelijke eisen van de Europese Commissie, die vormkrijgen in de AI Verordening (Europese Commissie 2021). Daarnaast ontwikkelt het kabinet richtlijnen, ontwerpprincipes en impact assessments, die moeten helpen om vooraf risico's in kaart te brengen en tegen te gaan (Kamerstukken II, 2019-2020, 26643, nr. 641). Projecten, zoals Calculemus-Flint, moeten bovendien helpen om wet- en regelgeving op transparante wijze te 'vertalen' in algoritmen. Ook bepleit het kabinet structureler toezicht op de algoritmische overheidsbesluitvorming door betere samenwerking tussen met name de Algemene Rekenkamer, de Autoriteit Persoonsgegevens en de Auditdienst Rijk (Kamerstukken II 2019-2020, 35212, nr. 3). Ten slotte zit de Tweede Kamer ook niet stil. Zo is de vaste commissie Digitale Zaken opgericht, die de digitale overheid kritisch zal volgen.

4.2 Uitdagingen voor beleid en politiek

Hoewel de belangrijkste problemen omtrent algoritmische overheidsbesluitvorming op de agenda staan, blijft het een uitdaging om rechtsstatelijke principes in de praktijk te operationaliseren en te handhaven. Een papieren werkelijkheid dreigt te ontstaan. Zo concludeerde de Algemene Rekenkamer dat er op dit moment onvoldoende zicht is op de algoritmische systemen die worden toegepast binnen de overheid (ARK 2021). En hoewel er veel wordt gesproken over het verbeteren van toezicht, ontbreekt het nog aan eenduidige, praktische standaarden waaraan digitale systemen moeten voldoen.

Ook bestaat er onvoldoende democratische zeggenschap over algoritmische overheidsbesluitvorming (Rathenau Instituut, 2021c; 2020b). Vaak komen voorstellen voor de ontwikkeling van nieuwe AI-systemen niet als wetsvoorstel langs het parlement, en vindt er zodoende geen zorgvuldige toetsing plaats van essentiële criteria, zoals rechtmatigheid, uitvoerbaarheid en handhaafbaarheid. Uitvoeringsorganisaties hebben vaak de ruimte om binnen hun bevoegdheden AI-systemen te ontwikkelen en uit te proberen. Dat is problematisch als een AI-innovatie, zoals het Criminaliteits Anticipatie Systeem (CAS), mensenrechten onder druk kan zetten.

Ook wanneer het parlement wel heeft ingestemd met een wet die ruimte biedt aan AI-innovaties, is het moeilijk om gedurende de ontwikkeling en implementatie van een nieuw systeem een vinger aan de pols te houden – terwijl dat wel nodig is. Zo is de effectiviteit van 'slimme' systemen vooraf lastig in te schatten en treden er vrijwel altijd onvoorziene effecten op. Tot nu toe blijken de opbrengsten van digitale

overheidsinnovaties regelmatig tegen te vallen – alle hoopvolle beloften ten spijt (JRC 2019). Het parlement is ook vaak reactief: pas wanneer het uit de hand loopt, vindt er controle plaats. Ten slotte worden veel innovaties uitbesteed aan en gebouwd door grote commerciële bedrijven als Google en Apple. Het blijkt lastig om met deze bedrijven voldoende afspraken te maken en regels op te stellen. Dit zet het vermogen van de wetgever om de digitale samenleving vorm te geven nog verder onder druk.

Figuur 5 Overzicht van kwesties en politieke vragen over een behoorlijke digitale overheid

© Rathenau Instituut

4.3 Welke politieke keuzes liggen voor?

- Toets op proportionaliteit: De wetgever speelt bij een belangrijke rol in het toetsen van proportionaliteit en subsidiariteit om grond- en mensenrechten te beschermen. De maatschappelijke kosten (bijvoorbeeld verlies van privacy, of risico op datalekken, discriminatie) moeten opwegen tegen de maatschappelijke baten. Maar wanneer is dat precies het geval? Welke mate van bewijsvoering is nodig om de effectiviteit van AI-systemen te kunnen beoordelen? Welke alternatieven zijn voorhanden? Resultaten van rapporten, impact assessments en audits kunnen hiervoor beter worden benut. Lees meer in het bericht 'Zeven aandachtspunten voor de AI-verordening' (Rathenau

Instituut 2021d) en het bericht ‘Zeven acties voor verantwoord innoveren met AI’ (Rathenau Instituut 2020l).

- Verbeter de wettelijke inbedding van data, algoritmen en AI: Het up-to-date houden van wetgeving is een cruciaal instrument waarmee het gebruik van data, data-analyse en andere digitale innovaties in juiste banen geleid kunnen worden. Maar vaak komen digitale systemen niet als zodanig langs het parlement. Digitale systemen worden voor gebruik dus niet door het parlement gewogen en getoetst aan de eisen van behoorlijk bestuur en grond- en mensenrechten. Er is meer zicht nodig op de vertaling van algemene wettelijke voorschriften naar specifieke systemen, en op wie die maken: uitvoeringsinstanties, ontwikkelaars of Big Tech. Welke afspraken worden met hen gemaakt? Lees meer in onze notitie voor de Eerste Kamer: ‘Grip op algoritmische besluitvorming bij de overheid’ (Rathenau Instituut, 2021c).

- Behoud het vermogen om fouten te repareren: Dit vraagt om de ontwikkeling van flexibele IT-systemen en om overheidsorganisaties waarin ambtenaren fouten kunnen (en durven) aan te kaarten en te herstellen. Ook is het essentieel dat toezichthouders genoeg capaciteit hebben om misstanden op te sporen en overheidsorganisaties aan de wet te houden. Wie is het aanspreekpunt voor burgers als het misgaat? Lees meer in de notitie ‘Grip op algoritmische besluitvorming bij de overheid’ (Rathenau Instituut, 2021c).

5 Duurzaam digitaal

5.1 Stand van zaken

De overheid streeft naar een samenleving met een schone energievoorziening, die betaalbaar, betrouwbaar, veilig en ruimtelijk inpasbaar is, zo schetst ze in de Kamerbrief 'Rijksvisie marktontwikkeling voor de energietransitie' (Kamerstuk II, 2020-2021). Dit doel zal flinke eisen stellen aan het elektriciteitsnet. Het elektriciteitsnet moet namelijk onder meer voldoen aan een hogere stroomvraag en moet een meer decentrale en variabele energieproductie mogelijk maken. Het huidige elektriciteitsnet opwaarderen zal tijdrovend en kostbaar, maar wel noodzakelijk zijn, omdat we anders te maken krijgen met stroomstoringen en -uitval. Digitale middelen kunnen helpen de uitdagingen aan te gaan, mits ze verantwoord en slim worden ingezet (Rathenau Instituut 2020m). Daarom ligt hier een grote beleidsopgave.

Dat wordt ook door overheden onderschreven. Zowel op nationaal als op Europees niveau wordt de potentie van digitalisering voor de energietransitie erkend, en wordt beleid ontwikkeld dat het gebruik van data voor dit doel moet stimuleren (EZK 2019; Kamerstuk II, 2020-2021; EC 2019). Op verschillende niveaus wordt ook gewerkt aan wet- en regelgeving die de uitwisseling en de inzet van data moet faciliteren. Voorbeelden zijn de concept-Energiewet en het data-afsprakenstelsel van de energiesector (met specifieke procedures voor de uitwisseling van energiedata). Bij al deze initiatieven gaat veel aandacht uit naar privacy en (digitale) veiligheid en naar het stimuleren van vertrouwen in datadeelprocessen. Ook benadrukken deze initiatieven het belang van meer zeggenschap voor burgers, onder andere door meer regie over hun gegevens.

5.2 Uitdagingen voor beleid en politiek

Zowel in de concept-Energiewet als bij het afsprakenstelsel ligt de nadruk op data die ingezet worden voor vanuit het energiedomein gereguleerde processen, en in het bijzonder data uit de slimme meter. Voor het realiseren van de energietransitie zijn echter ook andere typen data van belang, zoals gegevens uit apparaten in bezit van consumenten. Denk aan omvormers van zonnepanelen en warmtepompen of elektrische auto's. De privacy- en veiligheidseisen die voor meterdata gelden, zijn niet van toepassing op dit soort apparaten van commerciële partijen. Dat brengt risico's mee voor eigenaren; energiedata kunnen inzicht geven in het doen en laten

van huishoudens, en zijn daarom gevoelig voor misbruik (zie ook Hoofdstuk 3: Robuuste digitale infrastructuur). Maar de zwakkere privacy- en veiligheidseisen zorgen ook voor kwetsbaarheden in het grotere energiesysteem (Demoed 2018). Ook normen op het gebied van datakwaliteit en interoperabiliteit gelden niet voor commerciële fabrikanten.

Daarnaast verandert de energietransitie het speelveld in de energiesector. Nieuwe, soms machtige technologiebedrijven maken er nu hun intrede. Autofabrikant Tesla is bijvoorbeeld ook actief als aggregatiedienst, die energieflexibiliteit (vraag- en aanbod) van klanten bundelt en beheert. En Google en Amazon zijn actief op de markt van energiemanagementsystemen en combineren data die ze zo ophalen, weer met andere databronnen en diensten. Door allerlei schaalvoordelen kunnen dit soort grote bedrijven te veel (data)macht concentreren, wat een eerlijke energiemarkt in de weg staat (Olsen 2019). De energietransitie kan alleen slagen als burgers zoveel mogelijk op gelijke voet mee kunnen doen. Helaas ontbreekt het hen doorgaans aan de benodigde middelen, kennis en vaardigheden: niet iedereen kan immers zonnepanelen aanschaffen om duurzaam energie op te wekken, of wordt wijs uit het complexe aanbod van energiediensten.

Ten slotte staat digitalisering soms juist op gespannen voet met de doelen van de energietransitie. Digitalisering kan zeker een bijdrage leveren aan duurzame technologieën, maar digitale toepassingen verbruiken ook energie. Een laptop moet van stroom worden voorzien en een datacentrum ook. Hoewel digitale technologieën door innovatie zelf steeds minder stroom verbruiken, lijkt deze efficiëntiewinst niet voldoende om de toename in het gebruik van digitale technologie te compenseren. Er liggen dus lastige keuzes voor, die nog onvoldoende op de agenda staan van de overheid. Ook ontwikkelaars van datatoepassingen moeten zich meer bewust worden van de energievereisten van hun methoden. Sector en overheid willen doorgaans vooral verder digitaliseren, zonder de ecologische consequenties van die ambitie grondig te doordenken – en de digitale transitie in het perspectief van duurzame ontwikkeling te zien.

Figuur 6 Overzicht van kwesties en politieke vragen voor ‘duurzaam digitaal’

© Rathenau Instituut

5.3 Welke politieke keuzes liggen voor?

- Verbind digitalisering aan duurzaamheidsambities: Het is zaak dat de twee grote trends van deze tijd, digitalisering en verduurzaming, elkaar zoveel mogelijk versterken, en elkaar niet frustreren. Maar hoe? Duurzame digitale innovaties zijn belangrijk. Of zal een zekere afbouw van bepaalde digitale toepassingen, zoals data-intensieve processen, noodzakelijk zijn om de duurzaamheidsambities te halen? Een brede dialoog met alle betrokken partijen is nodig om zicht te krijgen op de voor- en nadelen van diverse opties. Lees meer in ‘Digitale infrastructuur verdient structureel aandacht’ (Masson en van Rooijen, 2021).
- Stel nadere eisen aan datadeling: Het slagen van de duurzame transitie vraagt om intensieve samenwerking tussen private partijen, overheden en burgers. Maar het is nog onvoldoende duidelijk hoe, op het gebied van datadeling, deze samenwerking vorm moet krijgen. Moeten consumenten bijvoorbeeld ook regie krijgen over data uit apparaten uit het commerciële domein, zoals slimme thermostaten, warmtepompen en elektrische auto’s? Welke beveiligingseisen

moeten daarvoor gelden (zie ook Hoofdstuk 3: Robuuste digitale veiligheid)? Moeten commerciële partijen gebruik maken van open standaarden? En in welke mate vinden politieke partijen het aan de overheid om dit te stimuleren? Europese wetsvoorstellen maken hiertoe al een eerste aanzet. Nederland kan ervoor kiezen een voortrekkersrol te spelen, bijvoorbeeld door de *Data Governance Act* (om data delen te stimuleren) en de *Digital Market Act* (gericht op dominante positie Big Tech) aan te scherpen. Lees meer in 'Verantwoord beheer van energiedata' (Rathenau Instituut 2020n).

- Randvoorwaarden om succesvol data te delen: Als burgers een actieve rol moeten spelen in het energiesysteem, moeten de randvoorwaarden daarvoor aanwezig zijn. Dat gaat verder dan alleen juridische kaders. Burgers hebben kennis van de energiemarkt en ICT nodig, en ze moeten beschikken over de financiële middelen om energieproducerende apparaten aan te schaffen. Wat mag er op dit vlak van burgers worden verwacht? Niet iedereen zal in gelijke mate in duurzame energie kunnen investeren. Welk flankerend beleid wordt ingezet om kansenongelijkheid tegen te gaan? Lees meer in het bericht 'Betrek burgers actiever bij de energietransitie' (Rathenau Instituut 2020o).

6 Hoogwaardig digitaal onderwijs

6.1 Stand van zaken

Het onderwijs heeft op allerlei manieren te maken met digitalisering (Rathenau 2020-2021). We richten ons hier op de opkomst van educatieve technologie. Daarmee bedoelen we enerzijds digitale leermiddelen, die leerlingen of studenten helpen om te leren. Denk aan oefensoftware, die leerlingen lesstof op hun niveau aanbiedt. Of aan een Virtual Reality-toepassing, waarmee een student in het beroepsonderwijs een moeilijke handeling alvast kan oefenen. Anderzijds doelen we met educatieve technologie op leermanagementsystemen. Dit zijn digitale systemen die allerlei administratieve zaken bijhouden, zoals ingeschreven leerlingen, cijferlijsten, studiedata, voortgang, absentie e.d.. Deze systemen worden steeds vaker integraal aangeboden. Daarbij zijn Nederlandse start-ups en educatieve bedrijven actief, evenals Big Tech bedrijven als Google en Microsoft.

De verwachting van scholen, bedrijven en beleidsmakers is dat educatieve technologie onderwijsinstellingen helpt om te innoveren: de technologie creëert nieuwe leermogelijkheden en zorgt voor een betere aansluiting op de veranderende, digitaliserende arbeidsmarkt en samenleving. In de afgelopen kabinetsperiode zijn diverse programma's opgetuigd om digitale innovatie in het onderwijs te stimuleren. Voorbeelden zijn het Versnellingsplan Onderwijsinnovatie (hoger onderwijs), saMBO-ICT (MBO), Slimmer Leren met ICT in het primair onderwijs en Leerling 2020 in het voorgezet onderwijs. Het onderwijs moet de achterstand op het gebied van digitalisering inhalen, was de gedachte. Ook in het Nationaal Groeifonds zitten projecten op het gebied van digitale innovatie en 'leven lang ontwikkelen'.

De stimuleringsprogramma's en ook de aanvragen in het Nationaal Groeifonds hebben aandacht voor risico's van digitalisering, zoals de bescherming van gegevens van leerlingen en studenten, onveilige systemen en de groeiende invloed van marktpartijen op het onderwijs. De vraag van de vele onderwijsinstellingen is versnipperd en het kan lastig zijn voor scholen om de goede systemen in te kopen, tegen een goede prijs. In 2018 werd daarom voor het primair en voortgezet onderwijs inkooporganisatie SIVON opgericht. Gaandeweg zijn de diensten van SIVON uitgebreid, door scholen ook hulp te bieden bij databescherming en internettoegang. De afgelopen jaren is het besef gegroeid dat digitalisering niet automatisch de kwaliteit van het onderwijs bevordert (Onderwijsraad 2017).

Door de coronapandemie is er nog meer aandacht gekomen voor de mogelijke gevolgen van digitalisering op het onderwijs. Door de noodgedwongen en snelle overstap naar digitaal leren werd bijvoorbeeld duidelijk welke aspecten van digitaal leren op afstand goed werken, en welke niet. Ook werd duidelijk dat het leren op afstand sommige leerlingen extra op achterstand zet en kan leiden tot kansenongelijkheid. Ook de privacyzorgen kregen een extra dimensie met de inzet van 'proctoring', software die studenten nauwlettend kan monitoren tijdens het maken van een toets of tentamen.

Tot slot kwam er meer aandacht voor de invloed van Big Tech. Grote technologiebedrijven deelden in de pandemie 'gratis' laptops uit en hun marktaandeel groeide aanzienlijk in zowel het lager als hoger onderwijs. Recent sloegen de ministers Van Engelshoven en Slob (2021) alarm over de dataverzameling van Google's *G-Suite for Education*. Scholen hebben beperkt zicht op wat er met deze metadata (gegevens over wanneer wordt ingelogd, welke functionaliteiten worden gebruikt e.d.) gebeurt en zijn afhankelijk van de voorwaarden van het bedrijf. Antwoorden worden gezocht in een betere naleving van de Algemene Verordening Gegevensbescherming en meer publieke regie over de inkoop van digitale systemen.

6.2 Uitdagingen voor beleid en politiek

De invloed van Big Tech gaat echter verder dan zeggenschap over onderwijsdata. Want ook als platformen data volgens de regels verwerken, kunnen zij hun producten met die data steeds verder verfijnen. Omdat Big Tech zoveel data verzamelen en toepassen, zetten ze concurrenten op een achterstand die vrijwel niet ingehaald kan worden. Ondertussen groeit de afhankelijkheid van onderwijsinstellingen van de totaalpakketten die grote technologiebedrijven aanbieden. Er dreigt een *vendor lock-in*. Private partijen kunnen dan ineens de prijzen verhogen, zoals onlangs gebeurde met het leerlingvolgsysteem Magister van Microsoft. Bovendien kan de afhankelijkheid leiden tot een verlies van zeggenschap over de *inhoud* en *kwaliteit* van onderwijs. Bieden de platformen bijvoorbeeld straks vooral winstgevende diensten, en is er minder ruimte voor diensten die leiden tot een evenwichtig curriculum?

Digitale innovatie in het onderwijs raakt zo aan een breed palet van publieke waarden. Naast gegevensbescherming en een eerlijke markt zijn ook waarden als autonomie, (sociale) rechtvaardigheid en menselijkheid in het geding. Door digitalisering – vaak gericht op efficiëntie en personalisering – verandert het onderwijs, ook als de digitalisering van in onderwijs onder publieke regie gebeurt en data goed beschermd zijn. Op dit moment is er nog weinig bekend over de

leeropbrengst van digitale middelen en hoe de leermiddelen het onderwijs en de kansen van leerlingen beïnvloeden. Komt er een te sterke nadruk op individuele en cognitieve ontwikkeling te liggen, ten koste van sociaal-emotionele ontwikkeling? Welke leerlingen kunnen goed uit de voeten met een beroep op meer zelfstandigheid en zelfmonitoring en welke niet? Durven leerlingen nog fouten te maken als elk leergedrag gemeten wordt? Er is dringend meer onderzoek nodig om deze vragen te beantwoorden. Digitalisering in het onderwijs vraagt om grote zorgvuldigheid.

Figuur 7 Overzicht van kwesties en politieke vragen over hoogwaardig digitaal onderwijs

© Rathenau Instituut

6.3 Welke politieke keuzes liggen voor?

- Publieke regie in de onderwijsmarkt: De scheve machtsverhoudingen in de digitale onderwijssector vinden steeds meer partijen een probleem. Welke mate van publieke regie is nodig om onwenselijke marktmacht en datamacht van grote technologiebedrijven tegen te gaan en voldoende zeggenschap van onderwijsinstellingen over de inhoud en kwaliteit van het onderwijs te behouden? Welke rol speelt het Ministerie van OCW als stelselverantwoordelijke, en welke taken moeten andere publieke instellingen

zoals SIVON en SURF vervullen? Leer meer in het bericht ‘Handvatten voor doordachte digitalisering in het onderwijs’ (Rathenau Instituut 2019c).

- De kwaliteit van digitaal onderwijs: De leeropbrengst van digitale leermiddelen, met name adaptieve leermiddelen, is nog onvoldoende helder. Stimuleer daarom onderzoek naar de leeropbrengst, waarbij niet alleen oog is voor cognitieve aspecten, maar ook voor de sociaal-emotionele ontwikkeling en het welzijn van leerlingen. Overweeg de invoering van uniforme en heldere kwaliteitseisen voor digitale leermiddelen. Lees meer in de serie ‘Leren digitaliseren’ (Rathenau Instituut 2020-2021).
- Scheppen van randvoorwaarden: Ten slotte vinden veel politieke partijen het belangrijk om de kansenongelijkheid in het onderwijs terug te dringen. Maar wat betekent dat voor de omgang met digitale leermiddelen? Welke inzet van digitale innovaties bevordert de onderwijskansen van kinderen? Ook hier is onderzoek belangrijk. Daarnaast is het van belang dat de onderwijsinspectie alert is op de verandering van het onderwijs door digitale leermiddelen, bijvoorbeeld door andere manieren van toetsing, en wat de digitalisering van onderwijs betekent voor de toetsing van de kwaliteit van het onderwijs. Lees meer de serie ‘Leren digitaliseren’ (Rathenau Instituut 2020-2021).

7 Verantwoord medische data delen

7.1 Stand van zaken

In de zorg stond het digitaal delen van data de afgelopen jaren hoog op de agenda. Door de overheid, de wetenschap en het zorgveld werd toegewerkt naar het eenvoudig en efficiënt digitaal uitwisselen van medische gegevens, tussen zorgverleners onderling en tussen patiënten en zorgverleners. De verwachting was dat dit zou leiden tot betere zorg. Zo stuurde voormalig minister Bruins van het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) in november 2018 het document 'Data laten werken voor gezondheid – Een kwestie van gewaarborgd vertrouwen' naar de Tweede Kamer (Minister Bruins 2018), waarin wordt beschreven hoe digitale gezondheidsdata van meerwaarde kunnen zijn voor onze eigen gezondheid en die van anderen.

Het ministerie wilde met name meer regie geven aan patiënten over hun gezondheidsdata, en daarmee over hun gezondheid. In de vorige kabinetsperiode heeft dit geleid tot gezamenlijke afspraken tussen koepels van zorgaanbieders, IT-leveranciers, patiëntvertegenwoordigers en VWS. Ook wil het kabinet werken aan 'datasolidariteit': het benutten van digitale gegevens uit medische dossiers voor onderzoek waarmee de volksgezondheid en medische wetenschap is gediend.

Helaas verloopt het opzetten en reguleren van datadeelsystemen, ondanks fikse subsidies, lang niet vlekkeloos. Zo is de wens van VWS om per 1 juli 2020 te zorgen dat iedere burger zijn eigen gegevens digitaal kan inzien en beheren niet in vervulling gegaan. Maar dit blijft wel de ambitie. Bovendien stuit het delen van medische data op bezwaren. Zo heeft de Tweede Kamer de afgelopen jaren – mede naar aanleiding van rapporten van het Rathenau Instituut (2018b, 2019d, 2020p) – aandacht gevraagd voor de kwetsbaarheden in datasystemen, waardoor de privacy van patiënten in het geding kan zijn. Ook zijn er zorgen over vaak commerciële apps waarmee burgers hun lichaamsfuncties en gedrag monitoren. Daarmee komt namelijk steeds meer informatie over onze gezondheid buiten het medische domein, en in handen van andere overheden en commerciële partijen die de data gebruiken op een manier die de democratie en de rechtsstaat kan ondermijnen.

Na de intrede van het coronavirus ging de volledige aandacht van VWS uit naar het ontwikkelen van de corona-apps en recentelijk naar het coronapaspoort. Daarbij richtte VWS opnieuw alle pijlen op een digitale oplossing. Het Rathenau Instituut

raadde het kabinet aan om het gebruik van corona-apps niet als de kern van de oplossing te zien, maar te beoordelen in een breder perspectief op publieke gezondheid. Dat betekent onder andere oog houden voor het op peil houden van de capaciteit en middelen van de GGD's. De ontwikkeling van de app was te gehaast en er was onvoldoende aandacht voor alle relevante aspecten, zoals een overtuigende rechtvaardiging van het gebruik van de apps en de proportionaliteit. Bovendien was er een gebrek aan basismaatregelen, zoals duidelijk werd door de datalekken in de GGD-systemen. Verder waarschuwden wij voor een verregaande afhankelijkheidsrelatie die de overheid aanging met de private bedrijven Google en Apple (Rathenau Instituut, 2020q; 2020r). Ook tijdens de ontwikkeling van het coronapaspoort lijkt er weinig gebruik te zijn gemaakt van alle ervaringen die zijn opgedaan rond de PGO's (Rathenau Instituut, 2021e).

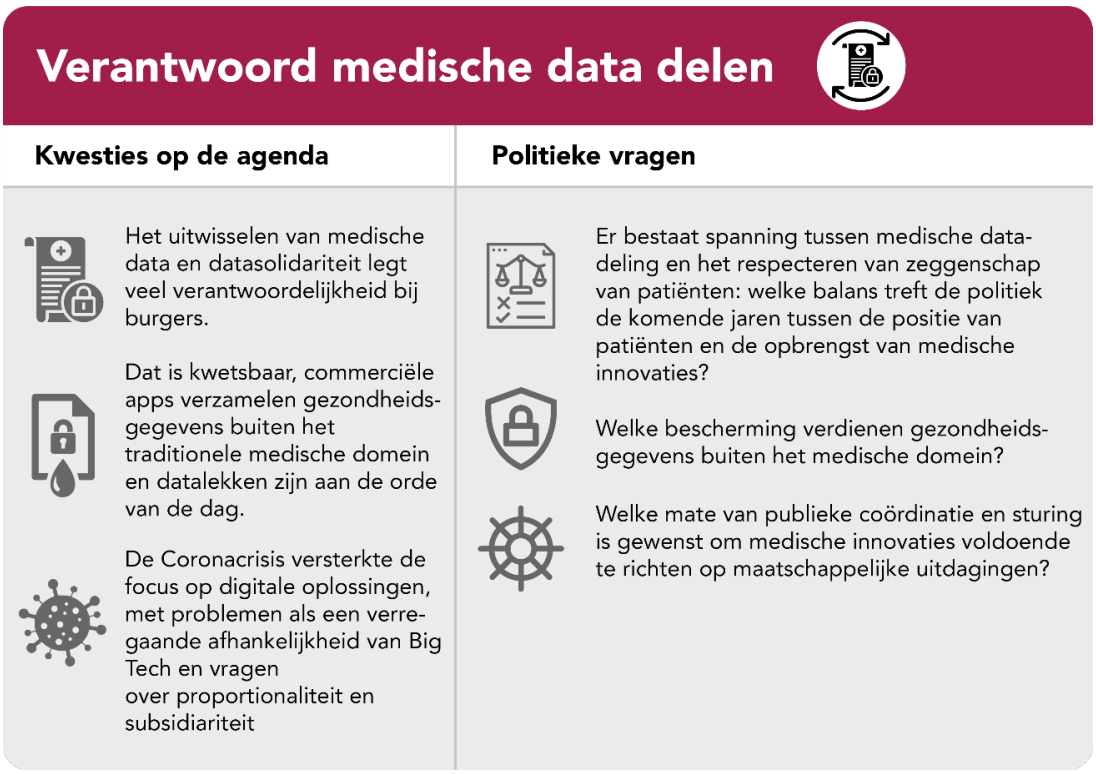
7.2 Uitdagingen voor beleid en politiek

De verwachtingen van het digitaliseren van medische data en het ontwikkelen van slimme zorg (eHealth, zoals digitale zorg op afstand) zijn te hoog: steeds denken de overheid, zorgverzekeraars en zorgverleners dat 'de app' of een digitale vorm van interactie tussen patiënt en arts soelaas zal bieden. Als gevolg daarvan wordt er een enorme druk op burgers gelegd om hun digitale gezondheidsgegevens beschikbaar te maken, in plaats van deze data proportioneel en onder verstandige voorwaarden te verzamelen. In de toekomst zal daarom gewerkt moeten worden aan dataprocessen waarbij burgers juist ondersteund worden om zelfstandig keuzes te maken over het delen van medische data en het gebruik van bepaalde apps.

Ook is het in de praktijk moeilijk gebleken om commerciële aanbieders, waaronder Big Tech bedrijven, voldoende te reguleren, terwijl die een steeds grotere rol van betekenis spelen in het medische domein. Private partijen hanteren nog steeds niet-transparante verdienmodellen en verkopen niet-transparante technische oplossingen. Zo doen algoritmische zorgsystemen aanbevelingen die dikwijls onbegrijpelijk zijn voor zorgprofessionals en daarmee de besluitvorming van zorgprofessionals niet ondersteunen, maar juist verwarren.

Je zou het als volgt kunnen samenvatten: ondanks de aandacht die er is geweest voor de ethische aspecten van een digitaliserende zorg, staat het vertrouwen van burgers in digitale medische innovaties, alsook de zeggenschap over hun eigen gezondheid en gezondheidsgegevens, onverminderd op het spel.

Figuur 8 Overzicht van kwesties en politieke vragen over verantwoord medische data delen



© Rathenau Instituut

7.3 Welke politieke keuzes liggen voor?

- Zet de gewenste zorg centraal: Te vaak staat de technologische belofte centraal, in plaats van concrete problemen in de zorg. Of is de wens om meer data te koppelen leidend. Beiden zorgen voor innovaties die niet aansluiten bij de wensen van professionals en patiënten. De inbedding in de medische praktijk en meer aandacht voor waarden als privacy, autonomie (om zelf te kunnen kiezen), toegankelijkheid en rechtvaardigheid (bijvoorbeeld bij systemen die gebruik maken van AI) is daarom cruciaal. Stimuleer nieuwe kennispraktijken waarin kennisinstellingen, bedrijven, gebruikers (professionals, cliënten en patiënten), beleidsmakers, regelgevers, burgers en/of andere relevante maatschappelijke partijen) gezamenlijk kunnen experimenteren met innovatieve oplossingen. Lees meer in ‘Gezondheid Centraal’ (Rathenau Instituut 2019d).

- Zorg voor de balans tussen zeggenschap en solidariteit: De afgelopen jaren werd duidelijk dat er een spanning bestaat tussen enerzijds de behoefte aan medische datadeling en innovatieve apps, en anderzijds de noodzaak om de rechten van patiënten te respecteren en hen zeggenschap te geven over hun medische data – inclusief de mogelijkheid om 'nee' te zeggen. Een overheid mag burgers niet te veel onder druk zetten. Tegelijkertijd is solidariteit van burgers wenselijk, zeker als het gaat om data die benut kan worden voor onderzoek ten behoeve van de volksgezondheid. Burgers kan gevraagd worden 'datasolidair' te zijn – mits de doelen voor onderzoek en ontwikkeling glashelder zijn, het delen van data plaatsvindt binnen het medische domein en de technologie zich bewezen heeft. Zo ontstaat balans tussen de positie van de burger en de maatschappelijke opbrengst van medische innovaties. Zie het rapport 'Datasolidariteit voor gezondheid' (Rathenau Instituut 2020p).

- Bescherm data buiten het traditionele medisch domein: Mede door digitalisering dijt het medisch domein uit en verzamelen tal van private partijen gezondheidsgegevens. De invloed van Big Tech groeit. Dit roept de politieke vraag op welke data precies de bescherming verdienen die in het medisch domein vereist is, en hoe private partijen aan die bescherming gehouden moeten worden. Bovendien is het van belang dat private medische innovatie voldoende gericht is op maatschappelijke uitdagingen, en publieke waarden een integraal onderdeel vormen van de ontwikkelprocessen. Dat vraagt om samenwerking en helderdere afspraken met de techleveranciers, mensen uit de praktijk, de artsen, verplegers en patiënten – en om innovatiebeleid dat coördinatie en sturing bevat. Lees ook het bericht: 'Een missie-gedreven aanpak voor slimme zorg en e-health' Rathenau Instiuut 2019e).

8 Betrouwbare immersieve technologie

8.1 Stand van zaken

Met de opkomst van technologie zoals Augmented Reality, Virtual Reality en spraaksystemen, raken we steeds verder ondergedompeld in de digitale wereld. Zo transporteert Virtual Reality ons naar een volledig kunstmatige wereld, waarin we bijvoorbeeld soldaten kunnen trainen op een virtueel slagveld. Augmented Reality voegt digitale lagen aan onze fysieke omgeving. Een automonteur kan met een slimme bril handige informatie zien terwijl hij naar de motor kijkt. Via spraaktechnologie kunnen we met computers praten en luisteren vele apparaten, zoals onze smartphones en slimme speakers, op steeds meer plekken met ons mee. Al deze technologische ontwikkelingen verknopen de fysieke en digitale wereld. Daarom noemen we AR, VR en spraaktechnologie ‘immersieve technologie’ (Rathenau Instituut 2020s; 2020t; 2020u; 2019f).

Immersieve technologie kan ingrijpende gevolgen hebben voor onze samenleving. Met nieuwe apparaten en diensten beschikken technologiebedrijven over nog meer data dan ze al deden, zoals gedrag, stem, oogbewegingen en gezichtsuitdrukkingen. Het wordt nog eenvoudiger om mensen in een openbare ruimte op afstand te identificeren. Hoe beschermen we privacy en anonimiteit op een adequate manier?

Spraaktechnologie en Augmented Reality maken het mogelijk een gezicht en stem te klonen en in een *deepfake* iemand iets te laten zeggen wat hij nooit heeft gezegd. Ook in Virtual Reality lopen echt en nep zo in elkaar over, dat mensen gaan geloven wat ze zien – en bijvoorbeeld verslaafd raken aan immersieve porno (Rathenau Instituut 2019f). Onze ervaring en onze waarneming kunnen als nooit tevoren geanalyseerd en gestuurd worden. Dat roept vragen op over de risico’s die burgers lopen, en over het handjevol machtige bedrijven dat immersieve technologie aanbiedt en consumenten beïnvloedt.

Toch vindt er op dit moment nauwelijks politieke discussie plaats over deze verknoping van de digitale en fysieke wereld. Hoe moet die hybride fysiek-virtuele wereld er uit zien en wie moet er betrokken worden bij het ontwerp ervan? De ontwikkeling van immersieve technologie ligt nu voornamelijk in handen van machtige technologiebedrijven. Zij ontwerpen de hybride wereld vanuit hun private belangen, terwijl een visie op het algemene belang ontbreekt.

Het is daarom de hoogste tijd voor publiek en politiek debat over de maatschappelijke inbedding van immersieve technologie. Een eerste stap is al gezet. Het Rathenau Instituut (2019f) riep de overheid al op om regulerende kaders te ontwikkelen voor de inbedding van VR, en deze oproep is door de Tweede Kamer overgenomen (Kamerstuk II, 2019-2020, 35 300 VI, nr 73). De minister heeft het Wetenschappelijk Onderzoeks en Documentatie Centrum (WODC) gevraagd te onderzoeken in hoeverre bestaande regulering en regelgeving afdoende zijn voor VR, AR en mixed reality (Kamerstuk II, 2019-2020, 26 643, nr. 689). Dit onderzoek inmiddels gepubliceerd (Schermer en van Ham).

8.2 Uitdagingen voor beleid en politiek

Op dit moment worden VR, AR en slimme speakers overwegend begrepen als gadgets. Gebruikers zijn voor bescherming tegen de risico's veelal overgelaten aan zelfregulering van de industrie, die met name gedragscodes heeft ontwikkeld. Deze zelfregulering is een positieve ontwikkeling, maar gaat niet ver genoeg. De gedragscodes zijn vooral ingegeven door codes voor bestaande media, zoals televisie of internet, terwijl immersieve technologie in belangrijke opzichten verschilt van bestaande media. Denk aan de intieme gegevens die verwerkt worden en de indringende ervaring waarin je wordt ondergedompeld. Bovendien is wetgeving en overheidssturing nodig om aan de in ons onderzoek gesignaleerde uitdagingen tegemoet te komen.

Die uitdagingen zijn talrijk. Omdat immersieve technologie voortdurend gevoelige, intieme data verzamelt, zoals een opname van onze stem, onze gebaren of ons gezicht, levert de technologie privacyrisico's op. Maar denk ook aan nieuwe vragen over eigendomsrecht: wie kan allemaal gebruik maken van de talloze opnames van jouw stem of afbeeldingen van je gezicht? Je stem en gezicht zijn van jou, maar er zullen steeds meer digitale klonen ontstaan. Welke bescherming verdienen die (Rathenau Instituut 2020u)?

Daarnaast kan immersieve technologie gebruikers flink verwarren. Kinderen die tijdens een experiment in VR met orka's hadden gezwommen, dachten later dat ze dit écht hadden gedaan. Het is inmiddels bekend hoe snel mensen geneigd zijn om robots en robotstemmen allerlei menselijke eigenschappen toe te schrijven, en zelfs affectie voor ze te voelen. Ten slotte zet immersieve technologie het gemeenschappelijke karakter van de publieke ruimte onder druk, omdat mensen de mogelijkheid krijgen om publieke ruimtes via een persoonlijke digitale bril te bekijken. Dit kan de sociale cohesie ondergraven. Ook kunnen AR-ontwikkelaars zoveel commerciële virtuele lagen en toepassingen op een publieke ruimte loslaten,

dat die niet meer een plek voor iedereen is. Er zijn dus tal van onderwerpen waar voor politiek debat en politiek handelen.

Figuur 9 Overzicht van kwesties en politieke vragen over betrouwbare immersieve technologie

© Rathenau Instituut

8.3 Welke politieke keuzes liggen voor?

- Maatschappelijk debat: In tegenstelling tot andere nieuwe technologieën, zoals sociale media, robotica en AI, bestaat er nauwelijks discussie over immersieve technologie, terwijl de maatschappelijke impact groot is. Welke nieuwe etiquette en regels zijn er nodig in een hybride wereld? Tot hoever willen we ons laten onderdompelen? Wat kan de samenleving zelf, en waar is politieke actie nodig? Een breed maatschappelijk debat kan helpen om daar helderheid over te krijgen. Hoeveel zijn politieke partijen bereid te investeren in langetermijnonderzoek naar de impact op gezondheid?
- Juridische kaders: Eenzelfde verkenning is nodig op het gebied van juridische kaders. Immersieve technologie heeft op tal van juridische domeinen een impact, van het eigendomsrecht tot privacykwesties. Stel duidelijke grenzen aan bijvoorbeeld het klonen van stemmen, maken van *deepnudes* of het op afstand kunnen identificeren van personen en hun gedrag in de publieke ruimte.

- Consumentenbescherming: Ontwikkelaars en verkopers van immersieve technologie hebben doorgaans een sterke machtspositie ten opzichte van de consument. Door de grote hoeveelheid data die zij verzamelen over de voorkeuren en eigenschappen van consumenten, ontstaat informatie-asymmetrie: de verkopers weten veel over de consument, maar de consument weet weinig over hen. Welke mate van bescherming van consumenten vinden partijen wenselijk?

In ons manifest gaan we dieper in op de invloed van Virtual Reality, Augmented Reality en spraaktechnologie. Lees daar meer over de genoemde punten: ‘Stel nu 10 ontwerpeisen aan de digitale samenleving van morgen’.

9 Conclusie

Het Rathenau Instituut deed de afgelopen jaren onderzoek naar de manier waarop de samenleving digitaliseert, en voerde hierover gesprekken met vele stakeholders. We deden dat in tal van domeinen, zoals het openbaar bestuur, de zorg, energie en het onderwijs. Dit onderzoek bundelt de inzichten uit onze publicaties over al deze domeinen. We selecteerden acht urgente politieke vraagstukken voor de komende jaren en brachten per domein de belangrijkste maatschappelijke en ethische kwesties, beleidsopties en voorliggende politieke keuzes in kaart. In dit concluderende hoofdstuk beschrijven we de stand van zaken van de digitale samenleving (9.1) en beschrijven we de huidige blinde blekken in onze omgang met digitale innovatie (9.2). Tot slot formuleren we drie aandachtspunten voor de volgende kabinetsperiode (9.3).

9.1 De stand van digitaal Nederland

Turbulent vaarwater voor de digitale samenleving
In een notendop: de stand van de digitale samenleving is op tal van aspecten zorgelijk. Datalekken, hacks en de verspreiding van desinformatie ondermijnen onze veiligheid en het democratisch debat. De energierekening van digitale innovaties loopt op, terwijl de samenleving klimaatneutraal moet worden. De groeiende datahonger van bedrijven, overheden en onszelf heeft geleid tot continue surveillance en beïnvloeding. De macht van Big Tech staat inmiddels niet alleen een eerlijke economie in de weg, maar heeft ook negatieve invloed op de arbeidsmarkt en arbeidsomstandigheden, leefbaarheid van steden, het democratische debat en de rechtsstaat.

De macht van Big Tech strekt zich uit tot alle acht voor dit rapport geselecteerde domeinen. De samenleving wordt voor essentiële diensten als videobellen, email en laptops in de klas steeds afhankelijker van de techleveranciers. Het ontbreekt regelmatig aan afspraken waarmee scholen, ziekenhuizen of overheden de bedrijven ter verantwoording kunnen roepen. De bedrijven kunnen eenzijdig de voorwaarden wijzigen: van de prijzen die gelden tot diensten die niet meer worden aangeboden. De Britse overheid werd al geconfronteerd met een tijdelijke blokkade van Google en Apple van haar corona-app. Ook scholen worden afhankelijker van de diensten van Big Tech, waardoor zij lastiger invloed kunnen uitoefenen op de inhoud en kwaliteit van het onderwijs. Deze ontwikkelingen zetten het vermogen

van scholen, ziekenhuizen en overheden om zélf vorm te geven aan digitale innovatie onder druk.

De problemen zien we ook terug in het parlement. Hoewel privacybescherming en gelijke behandeling mede door de toeslagenaffaire hoog op de agenda staan, blijft het een uitdaging om als parlement voldoende zicht te krijgen op de werking van overheidssystemen – zodanig dat het parlement daarop kan toetsen.

En tot slot betekent de opkomst van immersieve technologie – Virtual Reality, Augmented Reality en spraaktechnologie – dat de al bestaande uitdagingen van de digitale samenleving zich uitbreiden (zie hoofdstuk 8). Immersieve technologie verzamelt nóg intiemere gegevens, maakt het kinderspel om digitale beelden te manipuleren (*deepfakes* en *deepnudes* leiden nu al tot schadelijke gevolgen op individueel en maatschappelijk niveau) en biedt nóg meer mogelijkheden voor bedrijven om ons te volgen en te sturen.

Huidig beleid blijkt onvoldoende

De afgelopen jaren is in de samenleving het bewustzijn gegroeid dat digitalisering publieke waarden onder druk kan zetten. Beleidsmakers en politici erkennen de problemen en spannen zich in om de digitale uitdagingen te lijf te gaan. Zo formuleerde het kabinet de nationale digitaliseringsstrategie, het Strategische Actieplan AI en de beleidsbrief AI, mensenrechten en publieke waarden. Het kabinet bevordert de ontwikkeling van AI-innovaties die voldoen aan ethische richtlijnen en verantwoord datagebruik. Daarvoor zijn ethische codes en hulpmiddelen ontwikkeld. In de zorg- en energiesector zijn afsprakenstelsels voor het delen van data uitgewerkt en wordt geïnvesteerd in onderzoek en innovatie naar bijvoorbeeld slimme zorgsystemen en een flexibel en duurzaam energiesysteem.

Toch blijkt het onvoldoende. De macht en invloed van Big Tech is tijdens de coronapandemie enkel gegroeid. Wat betreft de bestrijding van desinformatie zijn vele partijen het eens dat de opgestelde zelfregulering onvoldoende effect heeft. En ook onze digitale netwerken zijn nauwelijks veiliger geworden. Een duidelijke illustratie daarvan kwam met de oproep van de MIVD december 2020: laat bij een vertrouwelijke vergadering voortaan de telefoon of tablet maar thuis – de kans op afluisteren en spionage is inmiddels te groot. De uitdagingen van de digitale samenleving zijn zeker niet opgelost.

9.2 Blinde vlekken in beleid

Versmalde discussie over publieke waarden
Ons onderzoek wijst een aantal oorzaken aan die het uitblijven van oplossingen voor de uitdagingen van de digitale samenleving ten minste mede verklaren. Zo versmalt de discussie over publieke waarden in de praktijk. Het zwaartepunt ligt op technische beheersingskwesties: op welke wijze beschermt en beveiligt het systeem persoonsgegevens? Of: Is er gecheckt dat er geen bias ontstaat? Dat zijn belangrijke vragen, maar ze zijn gericht op het voorkomen van bepaalde risico's, en gaan te weinig in op de ingrijpende invloed van digitale technologie. Digitale technologie kan bestaande relaties en praktijken wezenlijk veranderen, en die verandering moet nauwkeurig beoordeeld worden.

In het onderwijsdomein (zie hoofdstuk 6) zien we bijvoorbeeld hoe de inzet van adaptieve leermiddelen (lesstof op maat aanbieden via kunstmatige intelligentie) de manier van lesgeven, de manier van toetsen en de interactie in de klas verandert. Bovendien leggen de huidige middelen meer nadruk op individuele en cognitieve aspecten van leren, en minder op de sociaal-emotionele ontwikkeling. Ook lijken de leerlingen die er al goed voorstaan, het meeste van de digitale leermiddelen te profiteren. Wat betekent dat voor kansengelijkheid? Ook in de zorg zien we dat ondanks de aandacht voor privacy en veiligheid, zeggenschap en vertrouwen nog niet goed geregeld zijn.

Met andere woorden: óók systemen die veilig, privacyvriendelijk en non-discriminerend zijn, kunnen leiden tot een verstoorde relatie tussen leerling en leraar, arts en patiënt en ambtenaar en burger – als er niet gesproken wordt over *hoe* technologie de praktijk beïnvloedt, en wat daarbij wel en niet wenselijk is. Hoe technologie ingezet wordt is geen natuurwet: beleid, politiek, maatschappij kunnen daar invloed op uitoefenen. Juist daarom is een maatschappelijk en politiek debat zo belangrijk: hoe willen we dat digitale zorg en onderwijs eruit zien? Wie levert de infrastructuur daarvoor, en welke eisen stelt de wetgever aan de private dienstverleners op dit punt? Hoe, en tot hoever, moet de markt- en datamacht van Big Tech precies aan banden worden gelegd? Het zijn stuk voor stuk politieke keuzes – maar het debat gaat tot nu toe te weinig over deze invloed van digitale technologie. Het is een blinde vlek.

Onbewezen maatschappelijke opbrengst AI-innovaties
Daar komt bij dat de bijdrage van digitale technologie regelmatig wordt overschat, zeker als het gaat om AI-systemen die complexe sociale voorspellingen doen. Zo is het vooralsnog niet bewezen dat AI-systemen kunnen voorspellen of iemand een baan succesvol zal uitvoeren, of dat iemand fraude zal plegen. Zelfs van slimme advertenties gebaseerd op geautomatiseerde profielen is onduidelijk hoe ze precies

werken en wat je ermee kan bereiken. Het uitblijven van bewezen opbrengst heeft gevolgen voor de politieke en maatschappelijk afweging om technologie wel of niet in te zetten. Waarom duidelijk risicovolle digitale technologie inzetten als de opbrengst daarvan niet duidelijk is?

Voor alle digitale technologie geldt dat het uitmaakt in welke context de technologie wordt ingezet, en technologie moet niet worden beschouwd als een quick fix voor complexe problemen. Anders blijven de beloofde maatschappelijke opbrengsten uit. Niet voor niets roept de bekende wetenschapper Sheila Jasanoff op tot nederigheid in onze omgang met technologie. Steeds opnieuw moeten we volgens haar stilstaan bij de sociale gevolgen van technologie, wie er het meeste schade van kan ondervinden en wat alternatieven zijn die ook het maatschappelijke probleem zouden kunnen aanpakken.

In onderzoeken van het Rathenau Instituut, bijvoorbeeld naar delen van medische data, zien we steeds dat de sleutel tot succesvolle digitale innovatie ligt in een verstandige inbedding in de praktijk. Door niet alleen in een laboratoriumomgeving de innovatie te ontwikkelen, maar ook in de echte wereld na te gaan wat de effecten zijn van de digitale innovatie. Dat vereist de betrokkenheid van artsen, verpleegkundigen, patiënten, zorgverzekeraars, onderzoekers en technologieaanbieders. Voor het geloof dat digitale innovaties als vanzelf tal van maatschappelijke uitdagingen zullen oplossen, is gezien de huidige inzichten geen plaats meer.

9.3 Naar zeggenschap en vertrouwen

Drie speerpunten voor een nieuwe digitaliseringsstrategie
Niet alleen Nederland kampt met deze blinde vlekken. Over de hele wereld bereiden overheden strengere wetgeving voor, bijvoorbeeld op het gebied van ethische kunstmatige intelligentie, de macht van Big Techbedrijven, cyberveiligheid en verantwoord data delen. De verantwoordelijkheden van bedrijven, overheden, toezichthouders en burgers worden in deze wetten opnieuw bekeken en vastgelegd. Voor Nederland zijn met name de voorstellen van belang die de Europese Commissie heeft gepresenteerd: de AI-verordening, de *Digital Service Act*, de *Digital Market Act*, de *Data Governance Act* en de *Data Act*. Ze bieden kansen om hardnekkige problemen aan te pakken.

Het is aan het volgende kabinet en de nieuw opgerichte commissie Digitale Zaken om deze kansen te pakken. Overheid en parlement moeten nu de regie nemen om te zorgen dat digitale innovatie écht bijdraagt aan deze publieke waarden. De komende jaren zullen uitwijzen of politiek en samenleving weer grip krijgen op

digitalisering, of dat een écht veilige, duurzame, gezonde en menselijke digitale samenleving door onze vingers glipt.

We benoemen drie speerpunten voor een nieuwe digitaliseringsstrategie:

1. Krachtige kaders: het kabinet moet richting geven aan digitale innovatie: stel kaders, eisen en randvoorwaarden vast, met bijbehorend sterk toezicht.
2. Waardengedreven innoveren, gebaseerd op een kritisch parlementair debat: deze kaders moeten waardengedreven zijn, zodat de innovaties daadwerkelijk bijdragen aan de samenleving: een hoogwaardige gezondheidszorg, goed onderwijs en een veilige samenleving. Ze moeten daarom geformuleerd worden op basis van een inhoudelijk brede en kritische parlementaire discussie over gewenste en ongewenste effecten van digitalisering.
3. Zeggenschap voor de praktijk: tenslotte dienen deze kaders, en het gevoerde overheidsbeleid, de zeggenschap van professionals en burgers te vergroten: de inzichten van leraren, dokters en politieagenten die met digitalisering te maken hebben, moeten worden benut. En hun zeggenschap over digitale innovaties moet worden bevorderd.

1. Stel krachtige kaders vast

De samenleving moet er van op aan kunnen dat digitale technologie voldoet aan grondrechten en vastgestelde kwaliteitseisen. Dat digitale producten en diensten veilig, duurzaam, eerlijk en effectief zijn. Daarvoor is het zaak dat overheid en parlement die heldere kaders stellen en toezichthouders de naleving daarvan controleren. Het is in het bijzonder van belang om normen af te dwingen bij Big Tech bedrijven, als dat nodig is om publieke waarden te beschermen.

Op dit moment zijn diverse nieuwe wettelijke kaders in de maak voor alle acht domeinen in dit rapport. Ze moeten de risico's van digitale technologie beperken – en ons voorbereiden op de volgende generatie digitale technologie: van 6G tot aan Virtual en Augmented Reality. De komende periode zullen de lidstaten onderhandelen over de voorgestelde pakketten. De vraag is natuurlijk: slagen we met de Europese voorstellen erin om de problemen van de digitale samenleving op te lossen?

Hoewel de voorgestelde wetgeving belangrijke kwesties agendeert, hebben ze diverse zwakke plekken. Neem de verspreiding van desinformatie en schadelijke content, zoals *deepfake*s en *deepnudes*. De AI verordening stelt een transparantieverplichting voor ten aanzien van *deepfake*s: de ontwikkelaar moet kenbaar maken dat het een *deepfake* betreft. Maar een slachtoffer van een *deepnude* zal daar in de praktijk weinig mee geholpen zijn. De AI verordening stelt ook een verbod op 'subliminale content' voor – maar vooralsnog is het onduidelijk of *deepfakes* en *deepnudes* onder dat verbod vallen. De *Digital Services Act* heeft

als doel illegale content tegen te gaan. Maar de voorgestelde transparantieverplichtingen gaan niet in op de detectie van *deepfakes*. Ook zijn er geen eisen om de snelheid waarmee illegale content zich kan verspreiden tegen te gaan.

Ook de voorgestelde *Digital Services Act* is op verschillende aspecten onduidelijk of beperkt. Zo gaan de transparantieverplichtingen niet in op de detectie van *deepfakes*, op het verminderen van de snelheid van verspreiding van illegale inhoud, of op het inperken van politieke microtargeting. Bovendien is het de vraag of het toezicht wel op orde is, nu platformen gaan beslissen wat illegale of schadelijke content is.

Het is daarom zaak dat het kabinet en het parlement daadwerkelijk tot krachtige kaders komen en de behandeling van de diverse wetsvoorstellen aangrijpen om de verplichtingen te verhelderen en aan te scherpen.

2. Innoveer waardengedreven, gebaseerd op kritisch parlementair debat

Overheidsbeleid dient gevoed en gecontroleerd te worden door een kritisch parlementair debat over hoe publieke waarden worden gerealiseerd. Daarbij is het cruciaal om de hierboven genoemde blinde vlekken aan bod te laten komen. Publieke waarden zouden in de volle breedte bij het debat betrokken moeten worden, of het nu gaat om digitale leermiddelen in het onderwijs of de geautomatiseerde verzameling van patiëntgegevens. Daarnaast moet de beoogde maatschappelijke opbrengst van digitale innovaties op de parlementaire agenda worden gezet. Hanteer daarbij mensenrechten als leidende principes – niet als essentiële ondergrens, maar als kwaliteitscriteria van hoogwaardige publieke voorzieningen zoals een excellente gezondheidszorg, goed onderwijs en een veilige samenleving.

Om het parlementaire debat te laten slagen is ook meer zicht nodig op de keuzes die ontwikkelaars maken ten aanzien van publieke waarden, en op de voortgang van innovatieprocessen. Dat vereist allereerst dat belangrijke digitale innovaties zodanig in de wet verankerd worden, dat het parlement ze überhaupt kan toetsen. Nu is dat vaak niet mogelijk, omdat het gebruik van nieuwe systemen, zoals het Criminaliteits Adaptatie Systeem van de politie, geregeld wordt via bestaande wetten als de Wet Politiegegevens, de Uitvoeringswet AVG of de Algemene Bestuurswet. Zodoende vindt er voor specifieke toepassingen geen expliciete parlementaire toetsing plaats op essentiële criteria zoals rechtmatigheid, uitvoerbaarheid en handhaafbaarheid. Daarnaast is het belangrijk dat het parlement nut en noodzaak van digitale overheidssystemen tijdig evalueert, omdat de effectiviteit van digitale systemen vooraf niet altijd goed is in te schatten, en er

onvoorziene effecten op kunnen treden. Bij deze evaluaties is het zaak om van te voren vast te leggen wie waarvoor verantwoordelijk is als er fouten optreden.

3. Creëer zeggenschap voor professionals en burgers

De onderzoeken van het Rathenau Instituut laten zien dat succesvolle innovatie tijd en inspanning kost. De sleutel ligt in een goede inbedding in lokale praktijken, en dan met name in het betrekken van de expertise van professionals. Te vaak echter, ligt bij innovatieprocessen de nadruk op de technologische belofte – het technisch werkend krijgen van de beoogde innovatie. Maar een innovatie is pas geslaagd als deze ook commercieel werkt, als die past binnen juridische kaders en als gebruikers, of zij die de gevolgen ondervinden, de innovatie omarmen. Daarvoor zijn ook nieuwe verdienmodellen, productieprocessen, regels, protocollen en routines van gebruikers nodig. Dit vergt nauwe samenwerking tussen regelgevende instanties, professionals op de werkvloer, vertegenwoordigers van het maatschappelijk middenveld en burgers.

Zeggenschap geven over digitale technologie betekent uiteindelijk dat de wetgever de rollen en verantwoordelijkheden van betrokken partijen helder vastlegt. Wat kunnen partijen zelf, waar is hulp van andere instellingen nodig, en welke randvoorwaarden zijn nodig? We geven een concreet voorbeeld: als een school overweegt een digitaal leermiddel aan te schaffen, welke informatie heeft het schoolbestuur dan nodig om een onderbouwde keuze te kunnen maken – bijvoorbeeld op basis van de verwachte leeropbrengst en de onderwijsvisie van de school. Waar kan de school die informatie vinden? Welke afspraken moet de school maken met de leverancier, waaronder grote bedrijven als Google? Is de school in de positie om die afspraken af te dwingen?

Tot slot

Het moge duidelijk zijn: politiek en samenleving staan de komende jaren voor een grote opdracht: zeggenschap en vertrouwen creëren zodat een inclusieve digitale democratie, een eerlijke data-economie, hoogwaardige digitale middelen voor zorg, onderwijs en bestuur, en een duurzame digitale samenleving ontstaan. Dat vraagt om het organiseren van responsiviteit bij de overheid: het blijven monitoren van technologische ontwikkelingen, maatschappelijke vraagstukken en blijven beoordelen welke kaders, eisen en rollen van diverse partijen in de samenleving nodig zijn. Het realiseren van publieke waarden is namelijk geen eenmalige exercitie, maar vraagt voortdurend om aandacht, politieke weging en keuzes.

Literatuur

Algemene Rekenkamer (2021) Aandacht voor algoritmes. https://www.rekenkamer.nl/publicaties/rapporten/2021/01/26/aandacht-voor-algoritmes.

Algemene Rekenkamer. (2019a). Digitale dijkverzwaring: cybersecurity en vitale waterwerken. https://www.rekenkamer.nl/publicaties/rapporten/2019/03/28/digitale-dijkverzwaring-cybersecurity-en-vitale-waterwerken

Algemene Rekenkamer. (2019b). Rijksoverheid heeft informatiebeveiliging en IT beheer nog niet op orde. https://www.rekenkamer.nl/actueel/nieuws/2019/05/15/rijksoverheid-heeft-informatiebeveiliging-en-it-beheer-nog-niet-op-orde

Cyber Security Raad (2021a) Integrale aanpak cyberweerbaarheid. Adviesrapport. https://www.cybersecurityraad.nl/adviezen/documenten/adviezen/2021/04/06/csr-adviesrapport-integrale-aanpak-cyberweerbaarheid

Cyber Security Raad (2021b) Nederlandse digitale autonomie en cybersecurity. Hoe verminderen we onze digitale afhankelijkheden met behoud van een open economie? https://www.cybersecurityraad.nl/adviezen/documenten/adviezen/2021/05/14/csr-advies-nederlandse-digitale-autonomie-en-cybersecurity---csr-advies-2021-nr.-3

Demoed, K. (2018) ‘Hacken van zonnepanelen kan leiden tot Europese stroomstoring‘. Website EenVandaag, 16 maart. https://eenvandaag.avrotros.nl/item/hacken-van-zonnepanelen-kan-leiden-tot - europese-stroomstoring/.

Europese Commissie (2019). *Clean energy for all Europeans*. Brussel: Europese Unie

Europese Commissie (2020). The Digitale Services Act Package. Zie https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

Europese Commissie (2021) Voorstel voor een Verordening van het Europees Parlement en de Europese Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (Wet op de Artificiële Intelligentie) en tot wijziging

van bepaalde wetgevingshandelingen van de Unie. https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52021PC0206&from=EN

Inspectie Overheidsinformatie en Erfgoed (2021). Een dementerende overheid 2.0? Een analyse over de informatiehuishouding bij het Rijk; 15 jaar “na een dementerende overheid?” https://www.inspectie-oe.nl/publicaties/publicatie/2021/02/09/een-dementerende-overheid-2.0

Hamer, J. en L. Kool (2021). Encryptie is noodzakelijk om alle burgers te beschermen tegen hacks. Opinie-artikel NRC. https://www.nrc.nl/nieuws/2021/03/15/encryptie-is-noodzakelijk-om-alle-burgers-te-beschermen-tegen-hacks-a4035599

Hurenkamp, M. & E. Tonkens (2019). ‘Democratie vernieuwen: iets minder geloof en wat meer argumenten graag’. Sociale Vraagstukken 20 april 2019.

JRC (2019) Exploring Digital Government transformation in the EU. Analysis of the state of the art and review of the literature. Publications Office of the European Union, Luxembourg

Kamerstuk II, 2019-2020, 26643, nr. 641 (brief van de minister voor Rechtsbescherming over waarborgen voor risico’s van data-analyse door de overheid).

Kamerstuk II, 2019-2020, 35212, nr 3 (Initatiefnota van het lid Middendorp: menselijke grip op algoritmen).

Kamerstuk II, 2019-2020, 35 300 VI, nr 73 (motie van de leden van der Straaij en van der Graaf over onderzoek aanpassing reguleringskaders Virtual Reality)

Kamerstuk II, 2019-2020, 26 643, nr. 689 (brief van de minister voor Rechtsbescherming dat het WODC onderzoek uitvoert naar juridische kader VR/AR en mixed reality).

Kamerstuk II, 2020-2021, 32813; 31239, nr. 536 (Kamerbrief ‘Rijksvisie marktontwikkeling voor de energietransitie’)

Masson, E. en G. van Rooijen (2021). Digitale infrastructuur verdient structureel aandacht. Opinie-artikel Het Parool. https://www.parool.nl/columns-opinie/opinie-digitale-infrastructuur-verdient-structureel-aandacht~b853b993/

Meer, T. W. G. van der (2018). ‘De participatie-elite en de participatieparadox.’Website Stuk Rood Vlees, 24 september 2018.

Minister Bruins (2018). Kamerbrief over data laten werken voor gezondheid. 15 november 2018.

Ministerie van Economische Zaken en Klimaat (2018). Nederlandse digitaliseringsstrategie.

Ministerie van Economische Zaken en Klimaat (2019). *Nederland Digitaal: De Nederlandse visie op datadeling tussen bedrijven*. Den Haag: Ministerie van Economische Zaken en Klimaat.

Ministers Van Engelshoven en Slob (2021). Kamerbrief Uitvoeren DPIA's in het onderwijs. 1 maart 2021.

NCBN (2020). Cybersecuritybeeld Nederland 2020. https://www.nctv.nl/documenten/publicaties/2020/06/29/cybersecuritybeeld-nederland-2020.

NCBN (2021) Cybersecuritybeeld Nederland 2021. https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021

OESO (2019) Recommendation of the Council on Artificial Intelligence. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

Olsen, B. (2019). 'Google, Amazon Seek Foothold in Electricity as Home Automation Grows'. The Wallstreet Journal, 27 januari. https://www.wsj.com/articles/google-amazon-seek-foothold-in-electricity-as-home-automation-grows-11548604800.

Onderwijsraad (2017) Doordacht digitaal. Onderwijs in het digitale tijdperk. https://www.onderwijsraad.nl/publicaties/adviezen/2017/05/09/doordacht-digitaal

Passchier, R. (2021). Artificiële intelligentie en de rechtsstaat. Over verschuivende overheidsmacht, Big Tech en de noodzaak van constitutioneel onderzoek. Den Haag: Boom Juridisch.

Powells, G, & M. Fell (2019). 'Flexibility capital and flexibility justice in smart energy systems'. *Energy Research & Social Science* 54, pp. 56-59.

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

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

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

Rathenau Instituut (2017d). Nooit gelopen race. Over cyberdreigingen en versterking van weerbaarheid. Den Haag (auteurs: Munnichs, G., M. Kouw & L. Kool).

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

Rathenau Instituut (2018b). Digitale gezondheidsregie. Meer gegevens, meer grip? Den Haag (auteurs: M.G.H. Niezen & P. Verhoef)

Rathenau Instituut (2019a). Griffiers en digitalisering – Naar een sterkere lokale democratie. Den Haag (auteurs: Keulen, I. van, I. Korthagen en P. Diederen).

Rathenau Instituut (2019b). Cyberspace zonder conflict – Op zoek naar de-escalatie van het internationale informatieconflict. Den Haag (auteurs: Hamer, J., R. van Est, L. Royakkers, met medewerking van N. Alberts).

Rathenau Instituut (2019c) Handvatten voor doordachte digitalisering in het onderwijs. Bericht aan parlement. https://www.rathenau.nl/nl/digitale-samenleving/handvatten-voor-doordachte-digitalisering-het-onderwijs

Rathenau Instituut (2019d). Gezondheid Centraal. Zorgvuldig data delen in de digitale samenleving. Den Haag: Rathenau Instituut (auteurs: Niezen, M.G.H., Edelenbosch, R., Van Bodegom, L. & Verhoef, P.).

Rathenau Instituut (2019e). Een missie-gedreven aanpak voor slimme zorg en e-health. Bericht aan parlement. https://www.rathenau.nl/nl/digitale-samenleving/een-missiegerichte-aanpak-voor-slimme-zorg-en-e-health

Rathenau Instituut (2019f). Verantwoord virtueel – Bescherm consumenten in virtual reality. Den Haag (auteurs: Snijders, D., S. Horsman, L. Kool, R. van Est)

Rathenau Instituut (2019g) Zo brengen we AI in de praktijk vanuit Europese waarden. Artikel. https://www.rathenau.nl/nl/digitale-samenleving/zo-brengen-we-ai-de-praktijk-vanuit-europese-waarden

Rathenau Instituut (2020a) Meer grip op digitalisering – Een internationale vergelijking van parlementaire werkvormen. Den Haag (auteurs: De Jong, R., I. van Keulen, L. van Hove & G. Munnichs).

Rathenau Instituut (2020b). Digitale dreigingen voor de democratie. Over nieuwe technologie en desinformatie. Den Haag (auteurs: Boheemen, P. van, G. Munnichs & E. Dujso).

Rathenau Instituut (2020c). Initiatieven voor digitale democratie op nationaal niveau – Een internationale vergelijking. Den Haag (auteurs: Jong, R. de, J. Janssen, P. Faasse & P. Diederen).

Rathenau Instituut (2020d) Desinformatie bestrijden, censuur vermijden. Bericht aan parlement. https://www.rathenau.nl/nl/berichten-aan-het-parlement/desinformatie-bestrijden-censuur-vermijden

Rathenau Instituut (2020e) Met digitale middelen besluitvorming verbeteren. Bericht aan parlement. https://www.rathenau.nl/nl/berichten-aan-het-parlement/met-digitale-middelen-besluitvorming-verbeteren

Rathenau Instituut (2020f). Cyberweerbaar met nieuwe technologie – Kans en noodzaak van digitale innovatie. Den Haag, Rathenau Instituut (auteurs: Boheemen, P. van, G. Munnichs, L. Kool, G. Diercks, J. Hamer & A. Vos)

Rathenau Instituut (2020g). De belofte van opgavegericht innovatiebeleid – Een analyse van Europees innovatiebeleid voor de Green Deal en kunstmatige intelligentie. Den Haag (auteurs: Hessels, L., S.Y. Tjong Tjin Tai en J. Deuten).

Rathenau Instituut (2020h). EU, zorg dat AI ons duurzamer, gezonder, vrijer en veiliger maakt. Reactie consultatie whitepaper AI van de Europese Commissie. https://www.rathenau.nl/nl/digitale-samenleving/eu-zorg-dat-ai-ons-duurzamer-gezonder-vrijer-en-veiliger-maakt

Rathenau Instituut (2020i) Online platformen, offline impact. Bericht aan parlement. https://www.rathenau.nl/nl/berichten-aan-het-parlement/online-platformen-offline-impact

Rathenau Instituut (2020j). Maak werk van opgavegericht innovatiebeleid. Bericht aan het parlement. https://www.rathenau.nl/nl/berichten-aan-het-parlement/maak-werk-van-opgavegericht-innovatiebeleid

Rathenau Instituut (2020k) 5G-debat behoeft meer diepgang. Bericht aan parlement. https://www.rathenau.nl/nl/berichten-aan-het-parlement/5g-debat-behoeft-meer-diepgang

Rathenau Instituut (2020l) Zeven acties voor verantwoorde AI innovatie. Bericht aan parlement. https://www.rathenau.nl/nl/berichten-aan-het-parlement/zeven-acties-voor-verantwoord-innoveren-met-ai#:~:text=Op%2012%20maart%202020%20vergadert,voor%20onze%20maatschappij%20en%20economie.

Rathenau Instituut (2020m). 'Waardevol digitaliseren voor de energietransitie' Essay in opdracht van de Raad voor de Leefomgeving en Infrastructuur. (auteurs: Masson. E, Dekker, R. en Q. van Est). https://www.rli.nl/sites/default/files/essay_1_waardevol_digitaliseren_voor_de_energietransitie_-_rathenau_instituut_-_def_0.pdf

Rathenau Instituut (2020n). Verantwoord beheer van energiedata. Artikel. https://www.rathenau.nl/nl/digitale-samenleving/verantwoord-beheer-van-energiedata

Rathenau Instituut (2020o). Betrek burgers actiever bij de energietransitie. Bericht aan parlement. https://www.rathenau.nl/nl/berichten-aan-het-parlement/betrek-burgers-actiever-bij-de-energietransitie

Rathenau Instituut (2020p). Rapport: Datasolidariteit voor gezondheid. Verbeterpunten met oog voor ieders belang. https://www.rathenau.nl/nl/maakbare-levens/datasolidariteit-voor-gezondheid

Rathenau Instituut (2020q). De coronacrisis vraagt om zorgvuldig handelen en democratisch debat. Bericht aan parlement. https://www.rathenau.nl/nl/berichten-aan-het-parlement/de-coronacrisis-vraagt-om-zorgvuldig-handelen-en-democratisch-debat

Rathenau Instituut (2020r). Overwegingen naar aanleiding van de Kamerbrief introductie "CoronaMelder". Bericht aan parlement. https://www.rathenau.nl/nl/berichten-aan-het-parlement/plannen-voor-coronamelder-vragen-om-verduidelijking

Rathenau Instuut (2020s). Stel nu 10 ontwerpeisen aan de digitale samenleving van morgen. Manifest. https://www.rathenau.nl/nl/manifest

Rathenau Instituut (2020t). Hoor wie het zegt – Handvatten voor het verantwoorde gebruik van spraaktechnologie. Den Haag (auteurs: Hamer, J., S. Doesborgh en L. Kool)
Rathenau Instituut (2020u). Nep echt – Verrijk de wereld met augmented reality. Den Haag (auteurs: Snijders, D., E. Masson, S. Doesborgh, R. Groothuizen & R. van Est).

Rathenau Instituut (2020-2021) Leren Digitaliseren. Blogserie 1-6. https://www.rathenau.nl/nl/digitale-samenleving/leren-digitaliseren-1

Rathenau Instituut (2021a) De toekomst van online platformen. Bericht aan parlement. https://www.rathenau.nl/nl/berichten-aan-het-parlement/de-toekomst-van-online-platformen

Rathenau Instituut (2021b). Groeifonds vraagt om zelfbewuste partnerschappen in kennis- en innovatieecosystemen. Artikel. https://www.rathenau.nl/nl/vitale-kennisecosystemen/groeifonds-vraagt-om-zelfbewuste-partnerschappen-kennis-en-innovatie

Rathenau Instituut (2021c) Algoritmische besluitvorming bij de overheid. De rol van de Eerste Kamer. Notitie ter ondersteuning van de Eerste Kamer werkgroep AI. https://www.rathenau.nl/nl/digitale-zeggenschap/grip-op-algoritmische-besluitvorming-bij-de-overheid-de-rol-van-de-eerste

Rathenau Instituut (2021d) Zeven aandachtspunten voor de AI-verordening. Bericht aan parlement. https://www.rathenau.nl/nl/berichten-aan-het-parlement/zeven-aandachtspunten-voor-de-ai-verordening

Rathenau Instituut (2021e) Zeven overwegingen voor de discussie over een Coronapaspoort. https://www.rathenau.nl/nl/berichten-aan-het-parlement/zeven-overwegingen-voor-de-discussie-over-een-coronapaspoort

Rathenau Instituut (2021f) Grip op de digitale samenleving van morgen. Bericht aan parlement. https://www.rathenau.nl/nl/berichten-aan-het-parlement/grip-op-de-digitale-samenleving-van-morgen

ROB (2021) Sturen of gestuurd worden. Over de legitimiteit van sturen met data. https://www.raadopenbaarbestuur.nl/documenten/publicaties/2021/05/25/advies-sturen-of-gestuurd-worden

Schermer, B. en J. van Ham (2021) Regulering van immersieve technologieën. WODC Rapport.

Staatscommissie parlementair stelsel (2018). Lage drempels, hoge dijken. Eindrapport. Boom Amsterdam.

Staatssecretaris Keijzer (2020). Voortgang Roadmap Digitaal Veilige Hard- en Software. Kamerbrief 14 december 2020.

TNO (2019) Quick scan AI in de publieke dienstverlening (eindpresentatie 8 april 2019). https://www.rijksoverheid.nl/documenten/rapporten/2019/04/08/quick-scan-in-de-publieke-dienstverlening.

Tweede Kamer der Staten-Generaal (2020). *Update vereist. Naar meer parlementaire grip op digitalisering*. Rapport van de Tijdelijke Commissie Digitale Toekomst (TCDT).

UNESCO (2020) Draft Recommendation on the Ethics of Artificial Intelligence. Ad Hoc Expert Group https://unesdoc.unesco.org/ark:/48223/pf0000373434

Von der Leyen, U. (2019). Speech in the European Parliament Plenary Session. Strasbourg, 27 November 2019.

WRR (2019). Voorbereiden op digitale ontwrichting. Rapport nr. 101. Den Haag (auteurs: Prins, J.E.J, E. Schrijvers, R. Passchier en M. de Visser). https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting

© Rathenau Instituut 2021
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
Drs. Maria Henneman - voorzitter
Prof. dr. Noelle Aarts
Drs. Felix Cohen
Dr. Hans Dröge
Dr. Laurence Guérin
Dr. Janneke Hoekstra MSc
Prof. mr. dr. Erwin Muller
Drs. Rajash Rawal
Prof. dr. ir. Peter-Paul Verbeek
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