Rathenau Instituut

Grip op de digitale samenleving van morgen

Bericht aan het parlement

De afgelopen jaren is de digitale samenleving in turbulent vaarwater terecht gekomen. Datalekken, hacks, verspreiding van desinformatie en de afhankelijkheid van Big Tech raken de samenleving: van de pandemiebestrijding tot vrije verkiezingen. Maatschappelijk debat en politieke besluitvorming over deze kwesties is dan ook urgent. De Tweede Kamer concludeerde vorig jaar dat zij te weinig grip had op digitale ontwikkelingen en de politieke kwesties die daaruit ontstaan. Daarom is de vaste commissie Digitale Zaken opgericht.

Het Rathenau Instituut is 35 jaar geleden opgericht om het parlement te ondersteunen bij de politieke oordeelsvorming over wetenschap, technologie en innovatie. Dit doen we door onderzoek te doen naar de stand van wetenschap en kennis en door middel van dialoog, waarbij we inzicht bieden in verschillende visies en standpunten. Het Rathenau Instituut heeft de tijdelijke commissie Digitale Zaken vorig jaar ondersteund, onder andere door onderzoek naar de werkwijze van andere parlementen. We helpen de leden van de commissie Digitale Zaken nu graag op weg, met een overzicht van politieke vraagstukken die de noodzaak van de commissie onderstrepen. Het Bericht laat ook zien hoe deze vraagstukken met elkaar samenhangen en waar het werkterrein van de commissie Digitale Zaken samenvalt met het werkterrein van andere Kamercommissies.

Inhoud

1. Inleiding: de noodzaak van de commissie Digitale Zaken

Digitale technologie is cruciaal voor economie en maatschappij

Leven zonder digitale technologie is voor velen nauwelijks meer voor te stellen. Smartphones, sociale media, platformen, slimme camera's en kunstmatige intelligentie – ze brengen ons in verbinding met anderen, maken werken op afstand of een gesprek met een docent of dokter mogelijk. Digitale technologie is onlosmakelijk verbonden met alle onderdelen van de economie en maatschappij: om tijdig cyberaanvallen te detecteren, vroegtijdig kanker op te sporen, of de balans in een duurzaam energienet te behouden. Maar digitale technologie is niet zaligmakend en geen *quick-fix* voor complexe maatschappelijke problemen. Met de inzet van digitale technologie alleen zijn de klimaatdoelen niet bereikt, of is kansengelijkheid in het onderwijs niet gerealiseerd. Bovendien grijpt digitale technologie op allerlei manieren in op levens van burgers – ze kan belangrijke publieke waarden in onze samenleving en democratie onder druk zetten.

Sinds de onthullingen van Edward Snowden en het Cambridge Analytica-schandaal is er in het publieke debat veel aandacht voor publieke waarden in relatie tot digitale technologie. Intensieve discussies zijn gevoerd over hoe 'ethische' en 'humane AI' eruit moet zien. Bedrijven, wetenschappers en internationale instituties als de OESO en UNESCO stelden ethische richtlijnen, principes en codes op. Die moeten er bijvoorbeeld voor zorgen dat algoritmen en digitale systemen niet discrimineren en transparante beslissingen nemen. Verder berichtten de media veelvuldig over hoever de macht van Big Tech reikt. Beleidsmakers buigen zich over de vraag welke verantwoordelijkheden bij platformen belegd moeten worden. Ondertussen groeide ook het ongemak over de grote afhankelijkheid van veelal buitenlandse – en niet-Europese – technologieleveranciers, resulterend in oplopende geopolitieke spanningen over de apparatuur van 5G-leverancier Huawei.

Van ethische codes naar wet

Na een periode van zelfregulering en het opstellen van ethische codes, werken overheden overal ter wereld nu aan de nadere juridische inkadering van digitale technologie, waarin verantwoordelijkheden van bedrijven, overheden en burgers worden vastgelegd. Ze zullen bepalend zijn voor hoe de digitale samenleving eruit gaat zien – op allerlei terreinen zoals de zorg, energie, onderwijs of de economie. Wat verwachten we van bedrijven, overheden, publieke instellingen en burgers? Welke keuzes maakt het Nederlandse parlement?

Ook de Europese Commissie bereidt omvangrijke wetsvoorstellen voor, op het vlak van AI, Big Tech, cyberveiligheid en het gebruik van data. De wetsvoorstellen zullen invloed hebben op terreinen als de zorg, het onderwijs, energie, openbaar bestuur, detailhandel en defensie. 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.

Investeren in technologie om koploper te worden

Nederland en Europa willen bovendien niet alleen technologie reguleren, maar ook koploper worden in het toepassen van nieuwe digitale technologieën. Er liggen plannen klaar om veel geld te investeren in kunstmatige intelligentie, kwantum computing en cloud computing, in Nederland bijvoorbeeld via het Groeifonds. Maar succesvolle innovatie vraagt om meer dan technologische vernieuwing. Onderzoek van het Rathenau Instituut laat zien dat de sleutel van waardevolle digitalisering ligt in het denken vanuit de maatschappelijke praktijk en het betrekken van alle relevante maatschappelijke actoren. Dat vraagt om verbreding van het innovatiebeleid.

De noodzaak van de commissie Digitale Zaken

Er zijn dus veel prangende vraagstukken die de komende kabinetsperiode om politieke besluitvorming vragen. De Tweede Kamer heeft daarom besloten tot de oprichting van de vaste commissie Digitale Zaken, 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.

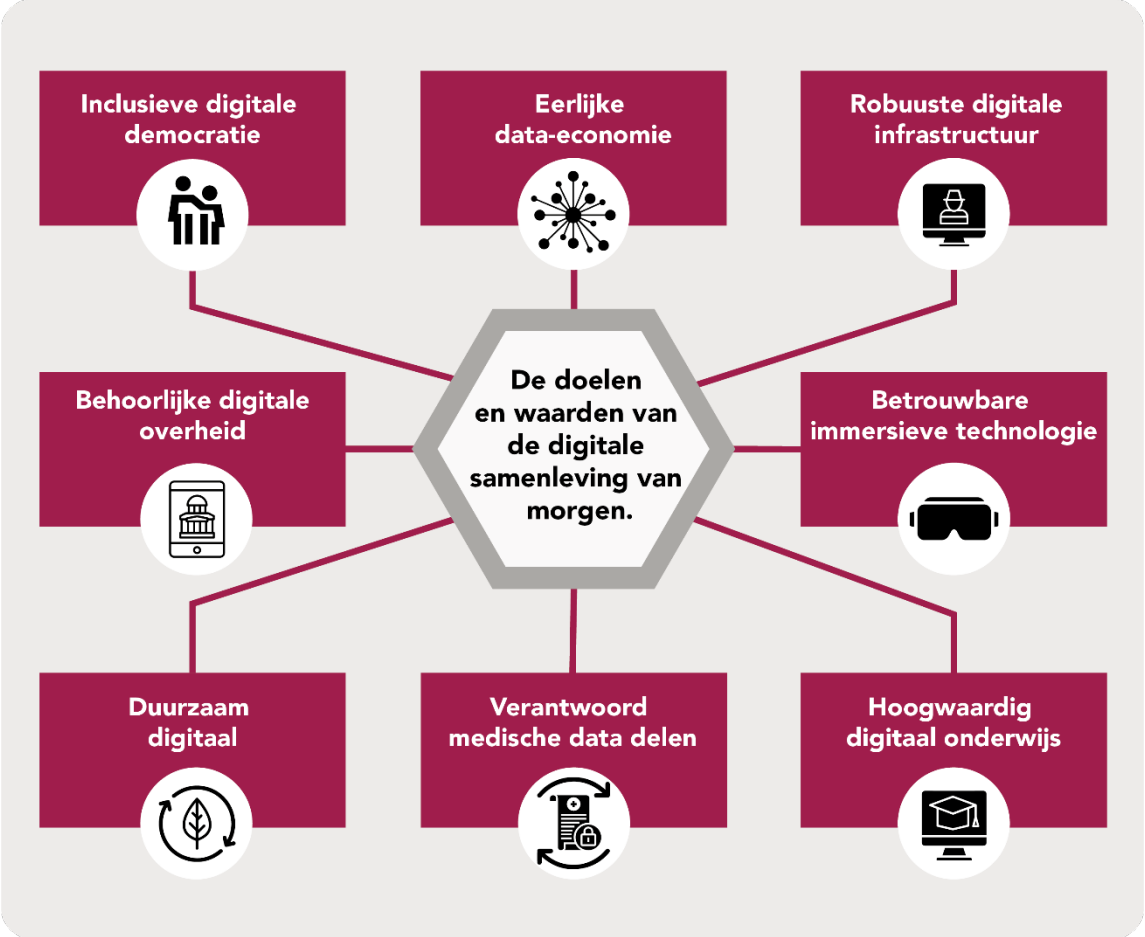
Naast hun rol in de *politieke besluitvorming*, kunnen de leden van de commissie Digitale Zaken een belangrijke rol spelen bij het tijdig *agenderen* en *doorgronden* van deze vraagstukken. Veel van deze vraagstukken hebben meerdere facetten en raken het werkterrein van meerdere commissies in het parlement. De leden van de commissie kunnen dus ook een belangrijke rol spelen bij een *integrale politieke behandeling* in het parlement, door te *coördineren* of te *adviseren* – nog een belangrijke reden waarom de commissie is opgericht.

Leeswijzer

Paragraaf twee geeft een overzicht van acht urgente vraagstukken waar het Rathenau Instituut een rol ziet voor de vaste commissie Digitale Zaken. Paragraaf drie laat de aard van de werkzaamheden op deze terreinen zien. We sluiten af met de boodschap dat grip krijgen op de digitale samenleving van de politiek vraagt om het organiseren van zeggenschap en het creëren van vertrouwen (paragraaf 4). Dat klinkt abstract, maar het betekent dat de komende jaren politieke besluiten nodig zijn, zodat taken en verantwoordelijkheden van verschillende partijen zijn vastgelegd, digitale innovaties aan kwaliteitseisen voldoen en in lijn zijn met grond- en mensenrechten, en zodat toezichthouders op de naleving daarvan kunnen toezien.

2. Overzicht van urgente vraagstukken

De afgelopen jaren heeft het Rathenau Instituut onderzoek gedaan naar de digitale samenleving. Op basis daarvan en gesprekken met breed scala aan stakeholders selecteren we acht domeinen die de komende jaren urgente politieke vraagstukken spelen (zie de figuur hieronder en Tabel 1). In de bijlagen beschrijven we voor elk van de acht vraagstukken 1) welke kwesties de afgelopen vier jaar op de beleidsagenda en politieke agenda zijn gekomen, 2) voor welke kwesties weinig aandacht is, en 3) welke politieke vragen voor liggen.



Tabel 1 Overzicht politieke vraagstukken

Domein	Vraagstukken
Inclusieve digitale democratie	Desinformatie, deep fakes, politieke micro-targeting en de macht van Big Tech bedreigen de democratie. Europese wetsvoorstellen voorzien in meer verantwoordelijkheden van platformen. Maar hoe ver reiken die verantwoordelijkheden? Tot hoever moet het gebruik van profilering aan banden worden gelegd? En welke mate van digitale middelen is gewenst om democratische besluitvorming en burgerparticipatie te versterken?
Eerlijke data-economie	Platformen brengen vraag en aanbod efficiënt bij elkaar, maar de enorme marktmacht, arbeidsomstandigheden en minder leefbare steden zijn daarvan keerzijden. Nieuwe wetten moeten de marktmacht reguleren. Nederland en Europa willen zelf koploper worden in digitale technologie. Maar met meer concurrentie ontstaat nog geen leefbare stad. En meer technologie lost maatschappelijke problemen niet vanzelf op. Welke plichten moeten platformen krijgen om een eerlijke en dynamische economie te realiseren? Wat betekent dat voor het vormgeven van innovatiebeleid – welke mate van sturing is wenselijk?
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. En nieuwe infrastructuren, zoals 6G en satellieten, komen eraan. Wat is er nodig om Nederland veiliger te maken, nu en in de toekomst? 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, 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? Welke mate van wettelijke inbedding is nodig om te waarborgen dat digitale overheidssystemen voldoen aan de eisen van behoorlijk bestuur?
Duurzaam digitaal	Digitalisering van het energiesysteem kan de energietransitie bevorderen. Wetsvoorstellen zijn gericht op een beter gebruik en uitwisseling van energiedata, met aandacht voor privacy en beveiliging. Maar steeds meer relevante data komt uit het commerciële domein, zoals slimme thermostaten of elektrische auto's. Grote bedrijven, zoals Tesla, vergroten bovendien hun invloed op de energiemarkt. Welke aanvullende kaders zijn nodig om data in dienst te stellen van de energietransitie? Bovendien kan digitalisering ook op gespannen voet staan met de doelen van de energietransitie. Welke keuzes liggen voor, en hoe weegt het parlement de opties?

Hoogwaardig digitaal onderwijs	Veel onderwijsinstellingen experimenteren met digitale leermiddelen. Op beleidsniveau is er aandacht voor dataprotectie, beveiliging en publieke regie over de inkoop van digitale systemen. Maar de impact van educatieve technologie reikt verder dan dat. Want wat betekenen de digitale 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 vanuit onderwijskwaliteit en publieke waarden?
Verantwoord medische data delen	Gebruik en 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 te gebeuren, en in het belang te staan van de publieke gezondheidszorg. Met de toename van het aantal 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 manipulatie te onderscheiden. De 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?

3. De aard van de werkzaamheden van de commissie Digitale Zaken

De in Tabel 1 genoemde vraagstukken beslaan het werkterrein van meerdere commissies in de Tweede Kamer. Daarom vereist het daadwerkelijk adresseren van de politieke uitdagingen een integrale behandeling van dossiers, concludeerde ook de Tijdelijke Commissie Digitale Toekomst (Tweede Kamer, 2020). De verspreiding van desinformatie raakt bijvoorbeeld niet alleen het waarborgen van vrije verkiezingen, wat onder Binnenlandse Zaken valt, maar houdt ook direct verband met het reguleren van platformen, een thema van Economische Zaken, en het tegengaan van illegale content, wat op het werkveld van Justitie en Veiligheid ligt. Voorliggende wetsvoorstellen vanuit de Europese Commissie, zoals de *Digital Services Act* en de *Digital Market Act* raken al deze beleidsterreinen.

De vaste commissie Digitale Zaken zal de komende tijd haar werkwijze bepalen. Het Rathenau Instituut geeft de leden van de commissie bij het bepalen daarvan een aantal volgende overwegingen mee. We noemen verschillende redenen waarom de commissie een rol kan spelen op een bepaald dossier.

Als vooruitkijken belangrijk is

De ontwikkeling van digitale technologie, zoals 6G of kwantumtechnologie, gebeurt doorgaans gedurende een langere periode. In het prille stadium is vaak nog geen politieke besluitvorming nodig, maar is het wel belangrijk om de voortgang te volgen en te weten wanneer en wat voor soort politieke vragen er aan komen, zodat politici zich daarop tijdig kunnen voorbereiden. Momenteel is Nederland bijvoorbeeld bezig met de uitrol van 5G, maar de standaarden en protocollen voor 6G worden nu bepaald. Die standaarden hebben invloed op bijvoorbeeld digitale beveiliging en gezondheid. Het is dus van belang dat volksvertegenwoordigers zich hier al op voorbereiden. Juist als er nog geen duidelijke politieke ‘probleemeigenaar’ is, kunnen de leden van de commissie Digitale Zaken de kwesties verkennen.

Als er sprake is van vergelijkbare vraagstukken of stakeholders

In publieke sectoren zoals de zorg, het onderwijs en energie liggen vergelijkbare vraagstukken op het gebied van data delen, dataprotectie, beveiliging en de groeiende invloed van platformen. Maar in al deze sectoren ligt sectorale wetgeving voor, die in aparte commissies behandeld. De commissie Digitale Zaken kan daarom een belangrijke coördinerende rol vervullen, om te leren van de aanpak in verschillende sectoren en *best practices* te signaleren, maar ook om te doorgronden welke knelpunten ontstaan en welke oplossingen voorhanden zijn. Bovendien geldt dat ook overkoepelende wetgeving, o.a. uit Europa, beoordeeld moet worden, die invloed heeft op alle sectoren. Welke mate van data delen is gewenst vanuit een goed functionerende markt én vanuit het oogpunt van de energietransitie, onderwijsdoelen en de volksgezondheid? De leden van de vaste commissie kunnen deze integrale afweging centraal stellen.

Naast de vergelijkbare vraagstukken kunnen ook de stakeholders betrokken bij bepaalde domeinen overeenkomen, zoals grote platformbedrijven die in het onderwijs,

de zorg en de energiesector actief zijn. Het zicht op de belangen van die partijen, en de impact van wetgeving op hen, kan door de behandeling in aparte commissies versnipperd raken. Het kan daarom een toegevoegde waarde hebben als de vaste commissie Digitale Zaken ook hier een coördinerende rol speelt.

Om zicht te houden op de samenwerking tussen toezichthouders

Toezichthouders hebben naast het parlement en de rechter een belangrijke rol in de manier waarop de samenleving grip houdt op digitale technologie. Digitalisering snijdt dwars door bestaande sectoren en juridische kaders heen. Zo raakt de verspreiding van desinformatie de terreinen van de Autoriteit Persoonsgegevens, de Autoriteit Consument en Markt en het Commissariaat van de Media. Digitale innovatie in de bankenwereld raakt de werkterreinen van onder andere de Autoriteit Financiële Markten, Autoriteit Consument en Markt en de Autoriteit Persoonsgegevens. De komende jaren wordt samenwerking tussen toezichthouders daarmee steeds belangrijker. En daarmee ook het zicht vanuit het parlement op de werkterreinen van de toezichthouders. De Tijdelijke Commissie Digitale Toekomst (Tweede Kamer, 2020) gaf al aan dat het van belang is om te zien waar gaten vallen, overlap ontstaat of aanvulling nodig is. De vaste commissie Digitale Zaken kan een belangrijke plek zijn om dit gesprek commissie-overstijgend te voeren.

4. Tot slot: grip vraagt zeggenschap en vertrouwen

Het werk van de vaste commissie Digitale Zaken is urgent. De digitale samenleving staat voor grote uitdagingen: van het verduurzamen van ons datagebruik tot het terugdringen van cybercriminaliteit. Parlementsleden zullen op tal van dossiers doortastend moeten optreden om zorgelijke trends te keren en digitale technologie te laten bijdragen aan maatschappelijke opgaven.

Daarbij is het cruciaal dat de zeggenschap over digitale technologie verstandig wordt georganiseerd. Dat betekent dat de wetgever de rollen en verantwoordelijkheden van betrokken partijen moet bepalen. We geven een concreet voorbeeld: als een school overweegt een digitaal leermiddel aan te schaffen, welke kennis heeft het schoolbestuur dan nodig over het dienstenaanbod? Welke afspraken moet de school maken met de leverancier, waaronder grote bedrijven als Google, om autonomie over het onderwijs te kunnen behouden? En is de school in de positie om die afspraken af te dwingen? Waar is hulp van andere instellingen nodig, of van de wetgever? Welke mogelijkheden en middelen hebben toezichthouders om op de afspraken toe te zien? De komende jaren is een belangrijke rol weggelegd voor de leden van de commissie Digitale Zaken om zeggenschap te creëren over digitale technologie en andere commissies hierbij te ondersteunen.

Uiteindelijk staat het vertrouwen van burgers in de digitale samenleving op het spel. Digitale innovatie bleek niet een wondermiddel voor maatschappelijke problemen, maar een even kansrijke als risicovolle technologische ontwikkeling. Digitale producten en diensten zullen veilig, duurzaam, eerlijk en effectief moeten zijn om het vertrouwen van

burgers in de digitale samenleving te behouden. Burgers moeten ervan op aan kunnen dat digitale technologie voldoet aan grondrechten en vastgestelde kwaliteitseisen. Met een overheid en parlement die heldere kaders stellen en toezichthouders die de naleving daarvan controleren.

Referenties

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

Rathenau Instituut (2020). Maak werk van opgavegericht innovatiebeleid. Bericht aan het parlement.

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

Bijlage 1: Inclusieve digitale democratie

1 – Het publieke en politieke debat: de 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 bijvoorbeeld op een ondoorzichtige manier beïnvloeden en het kan leiden tot een versplintering van het publieke debat. Het online publieke debat blijkt kwetsbaar te zijn voor manipulatie (Rathenau, 2020).

Digitalisering biedt tegelijkertijd nieuwe mogelijkheden voor interactie tussen burgers, politici en bestuurders. Maar digitale platforms en gadgets maken nog geen digitale democratie (Rathenau, 2018). 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 de polariserende werking van algoritmen op de platforms en de vatbaarheid van het publieke debat voor desinformatie en ongewenste buitenlandse beïnvloeding staan inmiddels hoog op de beleidsagenda. Het kabinet zette al in op 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 (Wpp) te herzien, met daarin aandacht voor manipulatieve digitale technieken zoals micro-targeting. Ook wordt invulling gegeven aan de Europese richtlijnen op het gebied van desinformatie (EU Action Plan on Disinformation).

De Europese Commissie bereidt strengere regelgeving voor over de macht en verantwoordelijkheden van platformen voor de verspreiding van misinformatie 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 deinsformatie tegen te gaan. Het vervangt het hier bovengenoemde, meer vrijblijvende, actieplan over desinformatie.

Tot slot zetten beleidsmakers in op het versterken en vernieuwen 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, 2019). 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, 2020).

2 – Welke problemen zijn blijven liggen?

Beleidsmakers richten zich 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 sociale mediaplatformen (ook de begrenzing van marktmacht speelt een rol, zie bijlage 2 Eerlijke data-economie). Een grote politiek 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. Het draait allereerst om politieke wil en verwachtingsmanagement over de doorwerking van inbreng van burgers in de formele politieke besluitvorming. 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 benutten voor de controlerende, agenderende en wetgevende taken van het parlement. Gemodereerde platforms voor interactie – van korte consultaties tot uitgebreide deliberaties – maar ook goede informatiesystemen die transparantie vergroten en informatie beter vind- en doorzoekbaar maken, kunnen de verbinding tussen burger, politiek en de overheid versterken. Dit vergt wel debat over wat de gewenste plek en rol van digitale democratische processen precies zijn. 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.

3 – Welke politieke vragen liggen voor?

- Bedreigingen van het politieke debat adresseren: tot hoever moeten de verantwoordelijkheden van platformen reiken? Zijn voorliggende wetsvoorstellen voldoende, of is meer nodig? Bijvoorbeeld ten aanzien van de verspreiding van schadelijke content, gepersonaliseerde advertenties, transparantie of risico op censuur? En moet het gebruik van persoonsgegevens van burgers verder aan banden worden gelegd? Welke grenzen zijn nodig ten aanzien van profilering?
- 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? En welke democratische processen zijn zo essentieel, in termen van bijvoorbeeld inclusie, menselijk contact en cybersecurity, dat analoge alternatieven nodig blijven?
- Eigen rol volksvertegenwoordiging: in hoeverre dient het parlement 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?

Referenties

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

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

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

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

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

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

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

Bijlage 2: Eerlijke data-economie

1 - Het publieke en politieke debat: de stand van zaken

Lange tijd werden vooral de voordelen voor consument en maatschappij gevierd van online platformen: 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.

De groeiende macht van de platformen van Big Tech, 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 Bijlage 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 Digitaliseringgstrategie (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 ingezet op zelfregulering in diverse sectoren, 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 2020).

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.

Vraag 2: Welke problemen zijn blijven liggen?

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 doel is om onderzoek en innovatie actiever te richten op het aanpakken van complexe maatschappelijke vraagstukken. Niet de technologische belofte staat dan 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 2020).

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 2021). Ook in haar Whitepaper on AI noemt de Commissie terreinen waarop AI kan bijdragen aan maatschappelijke uitdagingen, zonder te preciseren wat de uitdagingen zijn (Rathenau 2020). Ook kijken Europa en Nederland vooral naar publiek-private-samenwerking (PPS-constructies) 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 innovatie-agenda'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 Facebook's 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.

3 Welke politieke vragen liggen voor?

- Regulering van platformen: hoe kan bij voorliggende wetsvoorstellen 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 meer publieke regie nodig om semipublieke sectoren zoals onderwijs, gezondheid en energie vorm te geven vanuit publieke waarden?
- 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?

Referenties

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

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

Rathenau Instituut (2021). Online platformen, offline impact. Bericht aan het parlement.

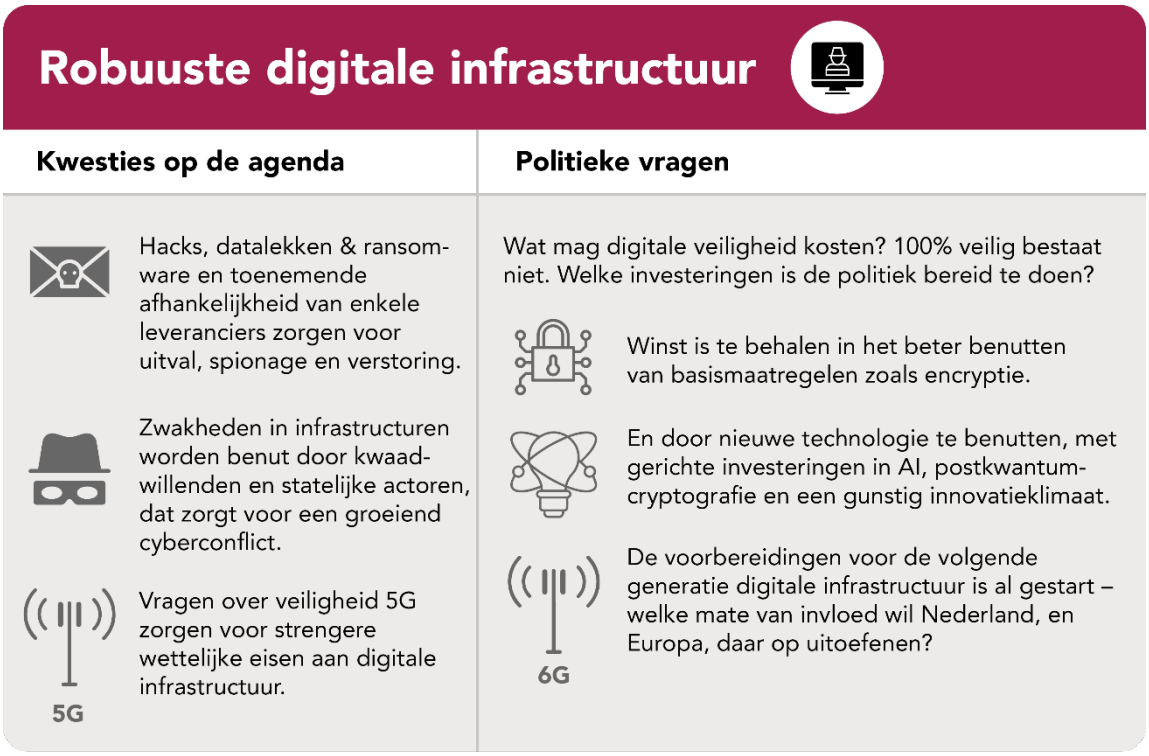
Rathenau Instituut (2020). Maak werk van opgavegericht innovatiebeleid. Bericht aan het parlement.

Rathenau Instituut (2020). EU, zorg dat AI ons duurzamer, gezonder, vrijer en veiliger maakt. Reactie consultatie whitepaper AI van de Europese Commissie.

Rathenau Instituut (2020). 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).

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

Bijlage 3: Robuuste digitale infrastructuur



1 – Het publieke en politieke debat: de stand van zaken

De digitale samenleving is een kwetsbare samenleving (Rathenau Instituut 2017; Rathenau Instituut 2020). 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 gebruikt worden voor spionage. Steeds weer blijkt dat de beveiliging van apparaten en diensten niet op orde is. Soms door menselijke fouten of het 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 regelmatig niet. 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 2019). 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 2020). 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.

2 – Welke problemen zijn blijven liggen?

Al deze inspanningen ten spijt, luiden instanties als de Algemene Rekenkamer (2019), de WRR (2019), Inlichtingendiensten (2020) en het Rathenau Instituut (2017, 2020) 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. Er rijzen vragen over handhaving en het actief invulling geven aan open normen in de nieuwe wetten. 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).

In Europa en Nederland tekent zich 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 aanwijzen van verantwoordelijkheden, het afleggen van verantwoordelijkheid en praktische veiligheidsstandaarden – zoals Europa dat in andere sectoren van de economie ook gedaan heeft (Von der Leyen 2019).

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.

3 – Welke politieke vragen liggen voor?

- Kosten van cyberweerbaarheid: investeringen in het cyberweerbaar maken van Nederland kosten geld. En 100% veilig bestaat niet. Welke risico's moeten zoveel mogelijk worden voorkomen, 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 strengere eisen aan vitale infrastructuur, diensten en aanbieders. In het energiedomein (zie ook bijlage 5: Duurzaam digitaal) geven we bijvoorbeeld aan dat privacy- en veiligheidseisen voor meterdata niet gelden op apparaten van commerciële partijen. Kansen liggen ook bij het benutten van nieuwe technologie, zoals kunstmatige intelligentie en postkwantumcryptografie. Welke gerichte investeringen zijn nodig om de Nederlandse expertise op dit vlak optimaal te benutten?

- 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 de politiek bereid te doen om 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?

Referenties

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

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

J. Hamer 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

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

Rathenau Instituut (2020). 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 (2019). 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 (2017). Nooit gelopen race. Over cyberdreigingen en versterking van weerbaarheid. Den Haag (auteurs: Munnichs, G., M. Kouw & L. Kool).

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

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

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

Bijlage 4: Behoorlijke digitale overheid

1 – Het publieke en politieke debat: de 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, 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. Het deed enorm veel stof opwaaien dat de overheid op grote schaal de rechten van burgers schond en jarenlang niet in staat bleek – of niet ter wille was – 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 uiteindelijk de rechter. 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 duidelijk 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 (). Daarnaast zet het kabinet in op de ontwikkeling van richtlijnen, ontwerpprincipes en impact assessments, die moeten helpen om vooraf risico's in kaart te brengen en te mitigeren (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 vaste commissie Digitale Zaken opgericht, die de digitale overheid kritisch zal volgen.

2 – Welke problemen zijn blijven liggen?

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 het op dit moment schort aan zicht 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, 2021; Rathenau Instituut, 2020). Vaak komen voorstellen voor de ontwikkeling van nieuwe AI-systemen niet als wetsvoorstel langs het parlement, en vindt er zodoende geen zorgvuldige toetsing plaats op 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. Het parlement is te 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.

3 – Welke politieke vragen liggen voor?

- Toetsen op proportionaliteit: de politiek speelt bij uitstek een rol in het toetsen op proportionaliteit en subsidiariteit om grond- en mensenrechten te beschermen. Maar wanneer wegen de maatschappelijke kosten (bijvoorbeeld verlies van privacy, of risico op datalekken, discriminatie) precies op tegen de maatschappelijke baten? Welke mate van bewijsvoering is nodig om de effectiviteit van AI-systemen te kunnen beoordelen? En welke mogelijke alternatieve oplossingen zijn voorhanden?
- Regulering 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 de juiste banen geleid kunnen worden. Maar welke wettelijke inbedding van digitale innovaties, in het bijzonder AI-systemen, is noodzakelijk om te zorgen dat zij voldoen aan de eisen van behoorlijk bestuur, en in lijn zijn met grond- en mensenrechten. Hier zal de politiek zich over moeten uitspreken.

Referenties

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

Tweede Kamer, vergaderjaar 2020–2021, 26 643, nr. 726.

Tweede Kamer, vergaderjaar 2019-2020, 26643, nr. 641.

Tweede Kamer, vergaderjaar 2019-2020, 35212, nr 3.

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

Rathenau Instituut (2020) Zeven acties voor verantwoorde AI innovatie. Bericht aan het Parlement.

Rathenau Instituut (2021) Notitie ter ondersteuning van de Eerste Kamer werkgroep AI: Algoritmische besluitvorming bij de overheid.

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.

Bijlage 5: Duurzaam digitaal

1 – Het publieke en politieke debat: de stand van zaken

De overheid streeft naar een samenleving met een schone energievoorziening, die betaalbaar, betrouwbaar, veilig en ruimtelijk inpasbaar is (Kamerbrief 'Rijksvisie marktontwikkeling voor de energietransitie', 2020). Dat zal flinke eisen stellen aan het elektriciteitsnet. Dat net 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. En dat brengt ons bij digitalisering. Want digitale middelen kunnen helpen de uitdagingen op te lossen, mits ze verantwoord en slim worden ingezet (Rathenau Instituut 2020a). 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 beleid ontwikkeld dat het gebruik van data voor dit doel moet stimuleren (zie bijvoorbeeld Nederland Digitaal, 2019; Kamerbrief 'Rijksvisie marktontwikkeling voor de energietransitie', 2020; Clean Energy for all Europeans, 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 (2020) en het data-afsprakenstelsel van de energiesector (met concrete 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.

2 – Welke problemen zijn blijven liggen?

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 Bijlage 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.

3 – Welke politieke keuzes liggen voor?

- Groene digitalisering: het is zaak dat de twee grote trends van deze tijd, digitalisering en verduurzaming, elkaar zoveel mogelijk versterken, en elkaar niet frustreren. Welke opties liggen daarbij op tafel? Is het vooral belangrijk om in te zetten op innovatie, 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. Maar het is aan de politiek om bij fundamentele keuzes knopen door te hakken.
- Eisen aan datadeling: het slagen van de duurzame transitie vraagt om intensieve samenwerking tussen private partijen, overheden en burgers. Maar de politieke vraag is 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? Moeten commerciële partijen gebruik maken van open standaarden? En in welke mate vinden politieke partijen het aan de overheid om dit te stimuleren?
- 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 verwacht worden? Niet iedereen zal in gelijke mate in duurzame energie kunnen investeren.

Referenties

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/.

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

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

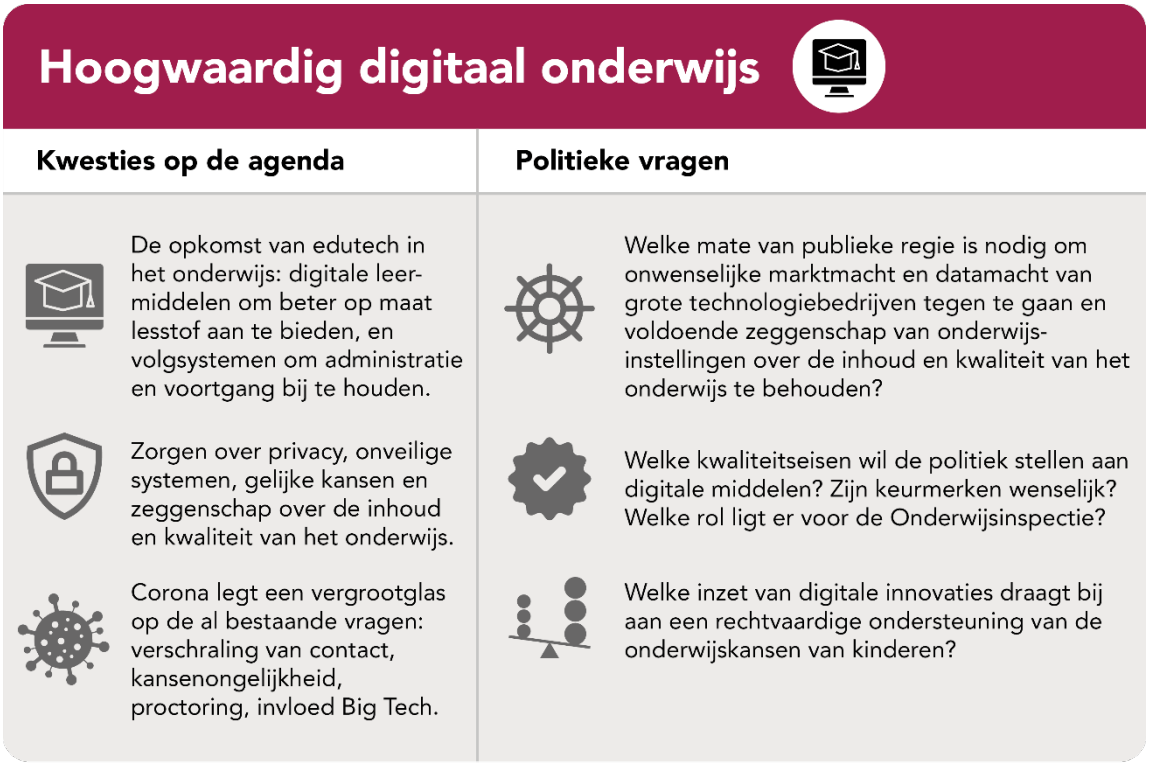
Kamerstuk II, 2020-2021, 32813; 31239, nr. 536 (Kamerbrief 'Rijksvisie marktontwikkeling voor de energietransitie')

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.

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

Rathenau Instituut (2020a). ‘Waardevol digitaliseren voor de energietransitie’ (essay in opdracht van de Rli). Website 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.

Bijlage 6: Hoogwaardig digitaal onderwijs



1 - Het publieke en politieke debat: de stand van zaken

Het onderwijs heeft op allerlei manieren te maken met digitalisering. 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 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 alarm over de dataverzameling van Google's *G-Suite for Education* (Ministers Van Engelshoven en Slob 2021). 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.

2 – Welke problemen zijn blijven liggen?

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 zo ongelofelijk veel 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 het onder publieke regie wordt uitgevoerd 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 bijvoorbeeld 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? 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.

3 – Welke politieke vragen 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?
- De kwaliteit van digitaal onderwijs: uniforme en heldere kwaliteitseisen stellen aan digitale onderwijsinnovaties is een manier om kwaliteit van digitale leermiddelen te borgen. Tot hoever moeten deze kwaliteitseisen reiken? En zijn keurmerken wenselijk? Ook zal gekeken moeten worden naar de rol van de onderwijsinspectie.
- 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?

Referenties

Digitalisering bedreigt onze universiteit. Het is tijd om een grens te trekken | De Volkskrant

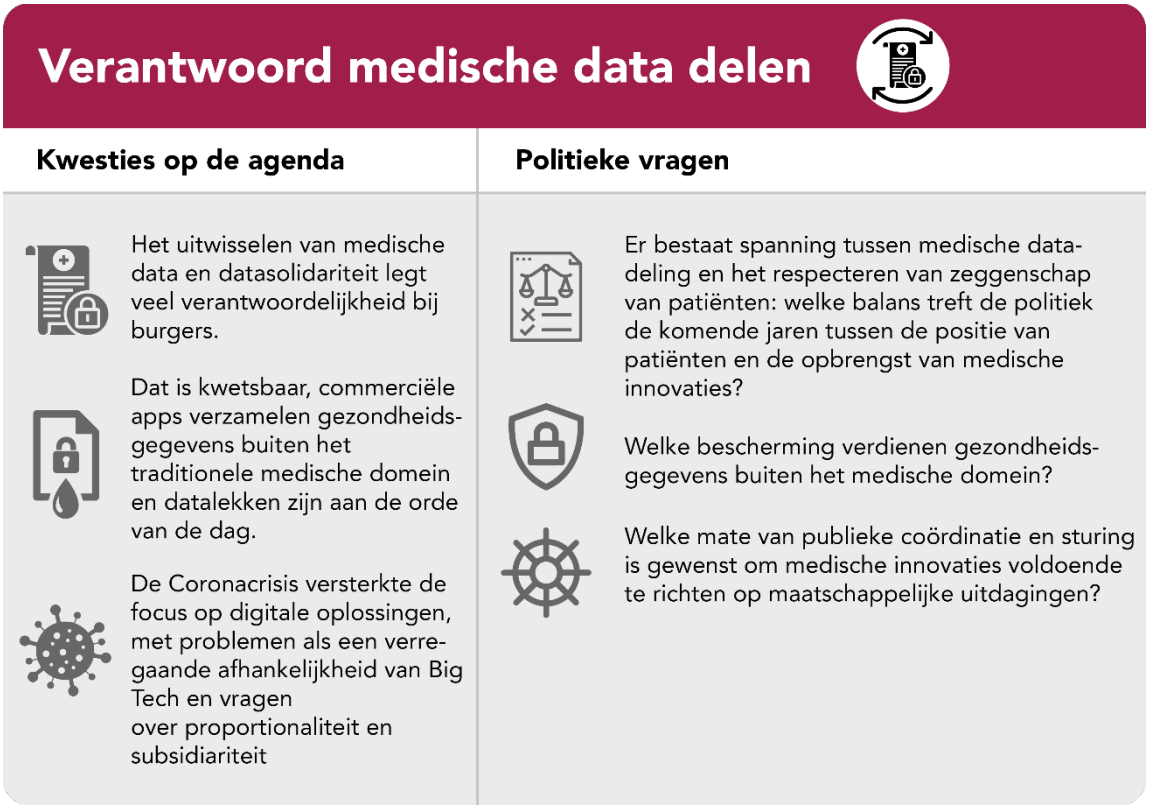
Onderwijsraad (2017) Doordacht digitaal.

Rathenau Instituut (2020-2021) Blogserie Leren Digitaliseren.

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

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

Bijlage 7: Verantwoord medische data delen



1 – Het publieke en politieke debat: de 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 (2018, 2019, 2020) – 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 rechtstaat 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, 2020). Helaas is eenzelfde weinig zorgvuldige houding zichtbaar bij de ontwikkeling van het coronapaspoort, waarbij alle ervaringen opgedaan rond de PGO's ongebruikt lijken (Rathenau Instituut, 2021).

2 – Welke problemen zijn blijven liggen?

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 gebruiken 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 de besluitvorming van zorgprofessionals niet ondersteunen maar 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.

3 – Welke politieke vragen liggen voor?

- 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 moet burgers niet te veel onder druk zetten, maar tegelijkertijd is solidariteit van burgers wenselijk, zeker als het gaat om data die benut kan worden voor onderzoek ten behoeve van de volksgezondheid. De politiek zal de komende jaren deze balans moeten vinden, met een scherp oog voor zowel de positie van de burger, als voor de maatschappelijke opbrengst van medische innovaties.
- Bescherming van data buiten het klassiek medisch domein: mede door digitalisering dijt het medisch domein uit en verzamelen tal van private partijen gezondheidsgegevens. 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.
- Groeiende invloed van Big Tech: nu digitale medische innovaties in grote mate door de private sector, waaronder Big Tech, worden ontwikkeld, rijst de vraag welke mate van politieke coördinatie en sturing nodig is, zodat private medische innovatie voldoende gericht is op maatschappelijke uitdagingen, en publieke waarden een integraal onderdeel vormen van deze ontwikkelprocessen. Hierbij is het ook van groot belang om duidelijk te maken welke samenwerking met mensen uit de praktijk, de artsen, verplegers en patiënten, nodig is om waardevolle innovaties tot stand te brengen.

Referenties

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

Rathenau Instituut (2021). Artikel: Het voorzorgsprincipe en digitale beslissingsondersteunende systemen in de zorg.

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

Rathenau Instituut (2020). Bericht aan parlement: De coronacrisis vraagt om zorgvuldig handelen en democratisch debat.

Rathenau Instituut (2020). Bericht aan het parlement: Overwegingen naar aanleiding van de Kamerbrief introductie "CoronaMelder".

Rathenau Instituut (2020). Artikel: Reactie op de ‘Verzamelwet gegevensbescherming’.

Rathenau Instituut (2019). Bericht aan parlement: Een missie-gedreven aanpak voor slimme zorg en e-health.

Rathenau Instituut (2019). Rapport: Gezondheid Centraal.

Rathenau Instituut (2019). Bericht aan parlement: Gegevensuitwisseling in de zorg.

Rathenau Instituut (2018). Rapport: Digitale gezondheidsregie.

Bijlage 8: Betrouwbare immersieve technologie

1 – Het publieke en politieke debat: de stand van zaken

Met de opkomst 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. Zo kan een automonteur 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 2020).

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 op een adequate manier? Spraaktechnologie en augmented reality maken het mogelijk een gezicht en stem te klonen en in een *deep fake* iemand iets te laten zeggen wat hij nooit heeft gezegd. Ook in virtual reality lopen echt en nep zo door elkaar heen dat mensen gaan geloven wat ze zien – en bijvoorbeeld verslaafd raken aan immersieve porno (Rathenau Instituut 2019). 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. In 2019 riep het Rathenau Instituut de overheid op om regulerende kaders te ontwikkelen voor de inbedding van VR (Rathenau Instituut 2019), en deze oproep is door de Tweede Kamer overgenomen (Kamerstuk 2020a). De minister heeft inmiddels 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 2020b).

2 – Welke problemen zijn er blijven liggen?

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 2020b)?

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.

3 – Welke politieke vraagstukken 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? 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 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. Zijn er grenzen aan bijvoorbeeld het klonen van stemmen, maken van *deep nudes* of het op afstand kunnen identificeren van personen en hun gedrag in de publieke ruimte? In hoeverre willen partijen nadere juridische eisen stellen aan techleveranciers?
- 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?

Referenties

Kamerstuk II 2019-2020a, 35 300 VI, nr 73.

Kamerstuk II 2019-2020b, 26 643, nr. 689.

Rathenau Instuut (2020). Manifest. Stel nu 10 ontwerpeisen aan de digitale samenleving van morgen.

Rathenau Instituut (2020). Hoor wie het zegt – Handvatten voor het verantwoorde gebruik van spraaktechnologie. Den Haag (auteurs: Hamer, J., S. Doesborgh en L. Kool)

Rathenau Instituut (2020). Nep echt – Verrijk de wereld met augmented reality. Den Haag (auteurs: Snijders, D., E. Masson, S. Doesborgh, R. Groothuizen & R. van Est).

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