

Rapport

Doordacht digitaliseren. Digitalisering doordacht

*Resultaten van een onderzoek naar het parlementaire debat
over digitaliseringsvraagstukken, 2009-2019*

Inhoudsopgave

Samenvatting	5
Inleiding	7
Hoofdstuk 1 Een digitale analyse van het parlementaire debat	9
Hoofdstuk 2 Vijf digitaliseringsvraagstukken nader onderzocht	15
Hoofdstuk 3 De informatiepositie van de Tweede Kamer	19
Hoofdstuk 4 De informerende, agenderende en regulerende rol van de Tweede Kamer	23
Hoofdstuk 5 Argumentatiepatronen in het parlementaire debat	27
Hoofdstuk 6 Een beoordelingskader voor de behandeling van digitale vraagstukken	31
Bijlagen	35

Dit onderzoek is uitgevoerd door Advies & Actualiteit – onderzoek in opdracht (A&A), een onderzoeksteam dat zich bezighoudt met actuele vraagstukken van maatschappelijke en (semi) overheidsorganisaties. Het team is verbonden aan de sectie Politieke Geschiedenis van de Radboud Universiteit. <http://adviesenactualiteit.ruhosting.nl>

Projectleiders: dr. Harm Kaal en dr. Carla Hoetink

Onderzoekers: Pepijn Aarnink MA MSc, dr. Carla Hoetink, Laura de Jong MA, dr. Harm Kaal, Lauren Lauret MA, Savannah Mellendijk BA

Ondersteuning digitale analyse: Lennart Kerkvliet, Arjen Swartsenburg, dr. Maarten Marx (Universiteit van Amsterdam)

Adviseurs: prof. dr. Carla van Baalen (Centrum voor Parlementaire Geschiedenis, Radboud Universiteit), prof. dr. Wim van Meurs (Politieke Geschiedenis, Research Institute for Culture & History, Radboud Universiteit), dr. Frans de Vijlder (Kenniscentrum Publieke Zaak, Hogeschool van Arnhem en Nijmegen)

Redactie: Susanne Geuze

Vormgeving: Studio Joyce Dekker

Bij voorkeur citeren als:

Kaal, Harm en Carla Hoetink, *Doordacht digitaliseren. Digitalisering doordacht. Resultaten van een onderzoek naar het parlementaire debat over digitaliseringsvraagstukken, 2009-2019* (Radboud Universiteit; Nijmegen 2020)

Het auteursrecht van deze publicatie berust bij de opdrachtgever: de Tweede Kamer der Staten-Generaal.

Samenvatting

In opdracht van de Tweede Kamer der Staten-Generaal hebben wij onderzoek gedaan naar het parlementaire debat over digitaliseringsvraagstukken in de periode 2009-2019. We hebben onderzocht welke lessen de Tweede Kamer kan trekken uit de manier waarop zij rondom deze vraagstukken de afgelopen jaren invulling heeft gegeven aan haar controlerende, wetgevende en volksvertegenwoordigende taak. Daarbij gaat het zowel om vraagstukken op het niveau van de overheid, als om de digitalisering in maatschappij en economie.

We ontleen deze lessen aan een analyse van het parlementaire debat in de afgelopen tien jaar. Door een combinatie van digitale analyse en kwalitatief onderzoek hebben we de inhoudelijke patronen en institutioneel-strategische keuzes in het debat over digitalisering blootgelegd. We hebben naar de volgende aspecten gekeken:

- De informatiepositie van de Tweede Kamer en de ontwikkelingen die hierin zijn opgetreden;
- De rol die de Tweede Kamer speelt in het debat over digitalisering: informerend, agenderend en regulerend;
- De argumentaties en dilemma's in het debat en de hierin gesignaleerde kansen en risico's ten aanzien van digitalisering.

Op basis van ons onderzoek trekken we de volgende conclusies:

- **De Tweede Kamer heeft afgelopen jaren een waardevolle rol gespeeld in het debat over digitaliseringsvraagstukken.**

Ons onderzoek laat zien dat de kring aan Tweede Kamerleden die zich actief met digitaliseringsvraagstukken hebben beziggehouden, klein is. Niettemin heeft de Kamer al vanaf de eerste debatten rond ICT/digitalisering – halverwege de jaren negentig – kwesties op de agenda gezet en zo mede richting gegeven aan het overheidsbeleid. Daarbij heeft ze gebruikgemaakt van een breed instrumentarium. *Dit biedt een goede basis om in de toekomst de grip op digitaliseringsvraagstukken te verstevigen.*

- **De meest effectieve Tweede Kamerdebatten over digitalisering worden vanuit publieke waarden gevoerd.**

Digitalisering is een autonoom en internationaal proces dat zich in hoog tempo voltrekt. Er komen complexe technologieën bij kijken, met velerlei (deels nog onbekende) toepassingsmogelijkheden. Deze realiteit draagt bij aan de indruk van de Tweede Kamer dat zij er onvoldoende grip op heeft. Commissievergaderingen en rondetafelgesprekken verhogen wel (incidenteel) het technologische kennisniveau, maar blijken minder aanknopingspunten te bieden om een politiek debat te voeren. *Publieke waarden bieden wel een dergelijk aanknopingspunt; ons onderzoek laat zien dat de meest effectieve parlementaire debatten op deze basis zijn gevoerd. Dit tilt het debat over digitalisering naar het niveau van een publiek en politiek vraagstuk.*

- **Het perspectief van economische kansen domineert het parlementaire debat over digitalisering, al heeft de Tweede Kamer steeds meer aandacht voor bepaalde risico's, met name ten aanzien van privacy en veiligheid.**

Al vanaf het midden van de jaren negentig kijkt de Tweede Kamer vooral naar digitalisering vanuit het perspectief van (economische) kansen. Toch heeft de Tweede Kamer ook in dit vroege stadium al oog voor risico's, met name zorgen rond privacy en veiligheid. Vanaf 2016 krijgen risico's in het

parlementaire debat meer aandacht, maar doorgaans nadat die zich in de praktijk hebben laten zien. *Vroegtijdig zowel kansen als risico's afwegen, en daarbij publieke waarden betrekken, bevordert de kwaliteit en slagkracht van het parlementaire debat over digitalisering.*

- **Het huidige parlementaire debat over digitalisering vindt versnipperd plaats.**
Digitalisering is een beleids- en domeinoverstijgende ontwikkeling. Het huidige parlementaire debat vindt verspreid over verschillende commissies plaats. Bovendien ontstaat het meestal ad hoc, bijvoorbeeld naar aanleiding van beleidsinitiatieven van de regering, maatschappelijke onrust of rapporten van onderzoeksinstellingen en adviesorganen. Een beperkt aantal digitaliseringsexperts in de Tweede Kamer voert daarbij het debat. Tegen deze achtergrond is het lastig voor de Tweede Kamer om een integrale kijk op digitalisering te ontwikkelen. *Door een gestructureerd debat te voeren, kan de Tweede Kamer de coördinatie van en controle op wetgeving en beleidsontwikkeling versterken.*
- **Het ontbreekt de Tweede Kamer regelmatig aan overzicht over de verschillende overheidspartijen en maatschappelijke organisaties die bij digitaliseringsvraagstukken betrokken zijn.**
Op wisselende wijze betreft de Tweede Kamer relevante overheidspartijen en maatschappelijke belanghebbenden bij het debat. De integraliteit van het debat over digitalisering omvat zowel het betrekken van relevante overheidspartijen (van de EU tot decentrale overheden en van landelijke toezichthouders tot uitvoeringsinstanties) als belanghebbenden (bedrijven, maatschappelijke belangenorganisaties). De Tweede Kamer kan haar eigen coördinerende en controlerende positie versterken, door deze partijen vroeg bij het debat en de beleidsontwikkeling te betrekken, of de regering hierop te controleren. *Het helder definiëren van de politiek-maatschappelijke dimensie van het voorliggende digitaliseringsvraagstuk helpt om te bepalen welke relevante belanghebbenden de Tweede Kamer moet betrekken bij haar gedachtenvorming. Heldere definiëring verbetert ook de integrale belangenafweging.*
- **De Tweede Kamer heeft digitalisering in het vizier en speelt inmiddels een belangrijke agenderende rol, maar is zoekende hoe zij een waardengedreven benadering kan omzetten in concrete beleidsmaatregelen en wetgeving.**
De Tweede Kamer heeft de afgelopen jaren met succes aangedrongen op de versterking van haar kennis- en informatiepositie ten aanzien van digitalisering. Daarbij speelt zij steeds meer een agenderende rol. Tegelijkertijd lijkt de Tweede Kamer te worstelen met de vraag hoe hieraan met concrete voorstellen vervolg te geven. In haar mede-beleidsbepalende en wetgevende rol is de Tweede Kamer kortom nog wat handelingsverlegen.

Om een concreet handelingsperspectief in beleids- en besluitvormingsprocessen te verkrijgen, kan een beoordelingskader uitkomst bieden. Tot besluit van dit rapport doen wij daarvoor een voorzet. Zo'n kader biedt de Tweede Kamer tevens houvast bij het doordenken van digitalisering als publiek en politiek vraagstuk, dat raakt aan de kerntaken van de volksvertegenwoordiging. Aan de hand van het beoordelingskader kan de Kamer beleidsterreinen die betrokken zijn bij een digitaliseringsvraagstuk in beeld brengen en doordenken, net als de gezagsstructuren tussen verantwoordelijke instanties en toezichthouders, relevante belanghebbenden, kansen en risico's, publieke waarden en ideologische aspecten.

Inleiding

In opdracht van de Tweede Kamer der Staten-Generaal hebben wij onderzoek gedaan naar het parlementaire debat over digitaliseringsvraagstukken. We hebben onderzocht welke lessen getrokken kunnen worden uit de manier waarop de Tweede Kamer in de afgelopen jaren invulling heeft gegeven aan haar controlerende, wetgevende en volksvertegenwoordigende taak. Deze lessen kunnen de Tweede Kamer helpen om haar grip op digitaliseringsvraagstukken te verstevigen. In dit rapport presenteren we de resultaten van ons onderzoek.

Digitalisering is een breed begrip. Het Rathenau Instituut (RI), dat onderzoek doet naar de maatschappelijke impact van wetenschap en technologie, typeert digitalisering in een van zijn recente rapporten als ‘een cluster van digitale technologieën die nu en in de komende jaren een plek zullen krijgen in onze samenleving’. Digitalisering is daarnaast ook een proces: ‘een enorme kracht [...] die de samenleving snel verandert’ en een ‘transitie [...] met kansen en risico’s’.¹

We benaderen digitalisering vanuit het perspectief van de overheid, in het bijzonder het perspectief van de Tweede Kamer. In ons onderzoek staat de periode 2009-2019 centraal, met de nadruk op de laatste vijf jaar.

Dit rapport begint met een overzicht van wat de Tweede Kamer zelf de afgelopen tien jaar onder digitaliseringsvraagstukken heeft verstaan (hoofdstuk 1). Ook bespreken we de centrale beleidsterreinen waarop de debatten over digitalisering plaatsvinden, en de Tweede Kamerleden die betrokken waren bij de debatten. Daarnaast brengen we in kaart welke initiatieven de regering ontplooid – zoals een reeks Digitale Agenda’s – en welke onderzoeksrapporten het parlementaire debat over digitalisering hebben gevoed.

Vervolgens introduceren we de vijf casestudies die we nader hebben onderzocht: de parlementaire debatten over Open Data, cybersecurity, eHealth, ICT in het onderwijs en SyRI (Systeem Risico Indicatie) (hoofdstuk 2). Deze casestudies geven inzicht in achtereenvolgens: de informatiepositie van de Tweede Kamer (hoofdstuk 3), de manier waarop de Tweede Kamer invulling heeft gegeven aan haar controlerende, wetgevende en volksvertegenwoordigende rol (hoofdstuk 4), en de koppeling van digitalisering aan politieke dilemma’s, kansen en risico’s (hoofdstuk 5).

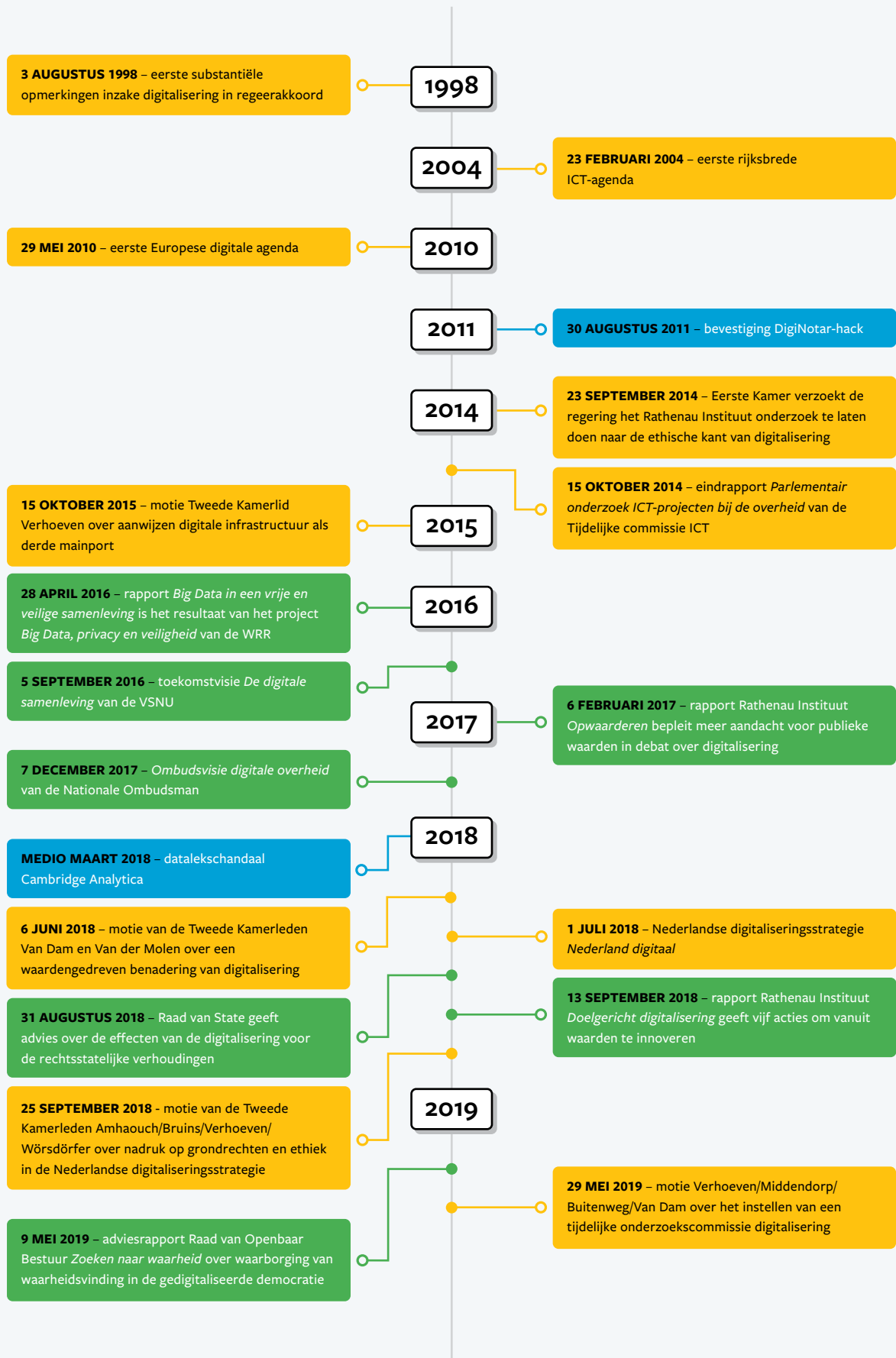
Uit de gecombineerde resultaten van de digitale en kwalitatieve analyse leiden we ten slotte een beoordelingskader af. Dit beoordelingskader kan de Tweede Kamer helpen om vroegtijdiger haar eigen positie te bepalen en bijdragen aan een grondige doordenking van digitaliseringsvraagstukken, met zowel oog voor de kansen als de risico’s (hoofdstuk 6).

Noot

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

Het digitaliseringsdebat

enkele mijlpalen



Hoofdstuk 1

Een digitale analyse van het parlementaire debat

In dit hoofdstuk presenteren we een selectie van een aantal inzichtgevende resultaten uit de digitale analyse die we hebben uitgevoerd over de periode 2009-2019, met enkele verkenningen verder terug in de tijd. Voor deze analyse hebben we samenwerking gezocht met computerwetenschappers van de Universiteit van Amsterdam. Zij hebben een nieuwe database van parlementaire documenten samengesteld voor de periode 2013-2019. Voor de periode tot 2013 konden we gebruikmaken van een bestaande database (search.politicalmashup.nl), aangevuld met gegevens uit de dataset parlementaire documenten op overheid.nl/official/publications. Op basis hiervan was het mogelijk om de verslagen van plenaire vergaderingen en commissievergaderingen integraal te doorzoeken en enkele, relatief eenvoudige, digitale en statistische analyses uit te voeren. In aanvulling hierop hebben we ook verkiezingsprogramma's, regeerakkoorden en overheidsagenda's onderzocht, om een beter beeld te krijgen van de recente geschiedenis van het politieke debat over digitalisering in Nederland.

De digitale analyse dient voor dit onderzoek vooral een signalerend doel. Met behulp van digitale tools hebben we ons een beeld gevormd van de manier waarop in het parlementaire debat inhoud en betekenis is gegeven aan digitaliseringsvraagstukken. Door woordwolken te genereren, hebben we een indicatie gekregen van woorden die de boventoon voerden in een bepaald Kamerdebat over digitalisering. Dat levert een eerste inzicht op in de verschillende typen vraagstukken, begrippen en waarden die raken aan het bredere begrip digitalisering. Ook woordfrequenties en frequenties van digitaliseringsdebatten zijn in kaart gebracht. Ten slotte hebben we geïnventariseerd welke fracties, Kamerleden en bewindspersonen bij deze debatten betrokken zijn geweest.

Het concept digitalisering, in de ruimste zin van het woord, vormde het vertrekpunt van dit onderzoek. Naast allerlei varianten van digitalisering (met de query `digit*`) betrof dit begrippen als ICT en computertechnologie. Om het woordveld rond digitaliseringsvraagstukken te inventariseren, hebben we vervolgens tal van zoekopdrachten uitgevoerd. Recente onderzoeksrapporten vormden hierbij een belangrijke inspiratiebron, net als het overzicht van debatonderwerpen dat de tijdelijke commissie ons aanreikte.

Uit deze verkenning blijkt dat politieke aandacht voor digitalisering een fenomeen is van de laatste twee decennia. Bij het parlementaire debat is een beperkt aantal Tweede Kamerleden betrokken geweest. Het perspectief van waaruit zij naar digitalisering kijken, heeft in deze relatief korte tijd belangrijke veranderingen ondergaan. Die veranderingen weerspiegelen het maatschappelijke debat – de groeiende zorgen over de invloed die digitalisering heeft op de samenleving en het leven van mensen, naast alle nieuwe mogelijkheden die het biedt.

Opkomst van digitalisering als politiek vraagstuk

Het gebruik van termen als digitalisering en ICT komt in het parlementaire debat op in de tweede helft van de jaren negentig. In het regeerakkoord van het tweede kabinet-Kok (1998-2002) is sprake van investeringen in de 'digitale snelweg', te beginnen met het onderwijs. In deze periode komen deze thema's ook voor het eerst in de verkiezingsprogramma's van politieke partijen voor. ICT/digitalisering

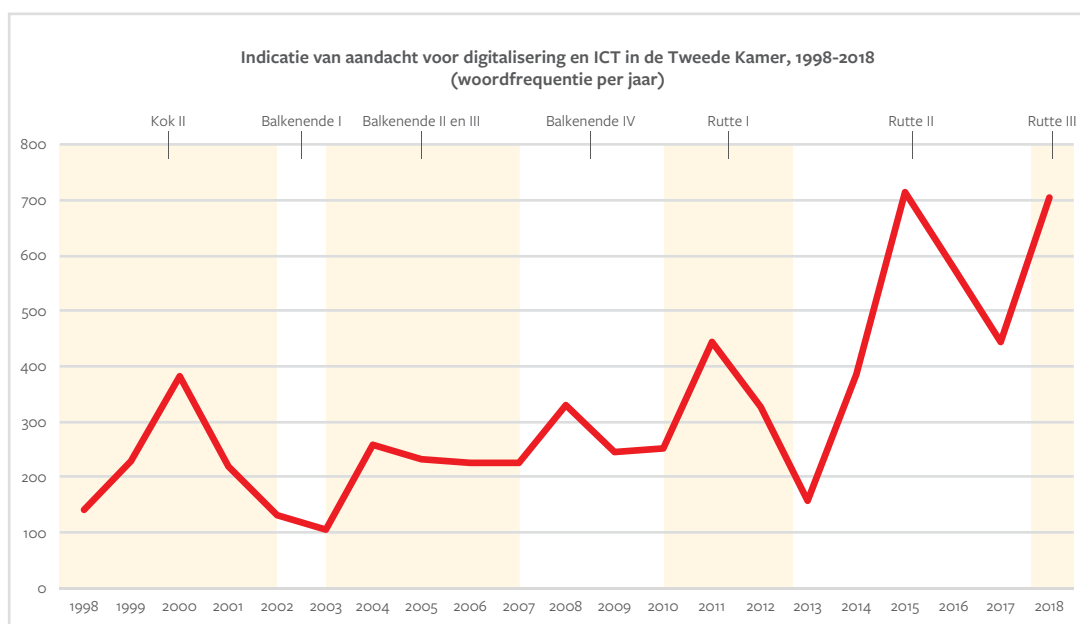
wordt rond 2000 door Tweede Kamer, regering en politieke partijen geassocieerd met economische groei en de ontwikkeling van nieuwe sociale netwerken. Ook risico's worden benoemd. Daarbij is aandacht voor bescherming van privacy en digitale grondrechten, en voor de noodzaak om in het onderwijs aandacht te besteden aan digitale vaardigheden.

Vanaf 2004 stelt de regering periodiek een ICT Agenda op (vanaf 2011 'Digitale Agenda' genaamd). In de eerste agenda stelt de regering dat ICT 'nog veel beloftes heeft waar te maken'.¹ De agenda, opgesteld door bewindspersonen van Economische Zaken, Bestuurlijke Vernieuwing en Onderwijs, Cultuur en Wetenschappen, legt de nadruk op kansen en mogelijkheden. In het Sociaal en Cultureel Rapport van 2004 is ook aandacht voor de risico's van ICT. Uit een enquête onder tweeduizend Nederlanders blijkt dat burgers zich vooral zorgen maken om cybercriminaliteit, aantasting van de privacy en *information overload*.² Rond 2012 neemt de aandacht voor digitale veiligheid en cybercrime toe.

In de loop der jaren breidt het aantal ministeries dat bij de agenda betrokken is zich uit, maar een economische benadering blijft lang dominant. In de agenda die de coördinerende minister van Economische Zaken in juli 2016 naar de Kamer stuurt, zet de regering uiteen 'hoe Nederland optimaal kan profiteren van de kansen (nieuwe toepassingen, verdienmodellen en banen) die deze mondiale transitie biedt'.³ In 2017 treedt een verschuiving op en zien we bij veel partijen in de verkiezingsprogramma's een afweging van kansen (Nederland als 'digitale mainport') en risico's, en meer aandacht voor de ethische vraagstukken die met digitalisering verbonden zijn, bijvoorbeeld rond robotisering.⁴ In 2018 introduceert de regering een nieuwe aanpak van het digitaliseringsbeleid; ze presenteert een reeks nieuwe digitale agenda's, met naast de koepelagenda NL DIGIbeter aparte agenda's voor cybersecurity (Nederlandse Cybersecurity Agenda) en (big) data (NL Digitaal - Data Agenda Overheid).

Digitalisering in het plenaire debat en de commissievergaderingen

Een frequentieanalyse van het parlementaire debat laat een geleidelijke stijging zien van het gebruik van het begrip digitalisering en daarmee samenhangende termen in het debat.



Woordwolken (zie hieronder) maken inzichtelijk dat deze termen verbonden zijn met debatten rond onderwerpen als cybersecurity, robotisering, de digitale overheid, hackers en de positie van het midden- en kleinbedrijf. Ook de betekenis van de omschakeling van fysiek naar virtueel contact, bijvoorbeeld in de communicatie tussen overheid en burger, komt in Kamerdebatten aan de orde. De woordwolken laten zien dat zulke debatten draaien om de vraag of burger en overheid meekunnen in de transitie van envelop naar digitale post en of het stelsel bestand is tegen hacks en malware.

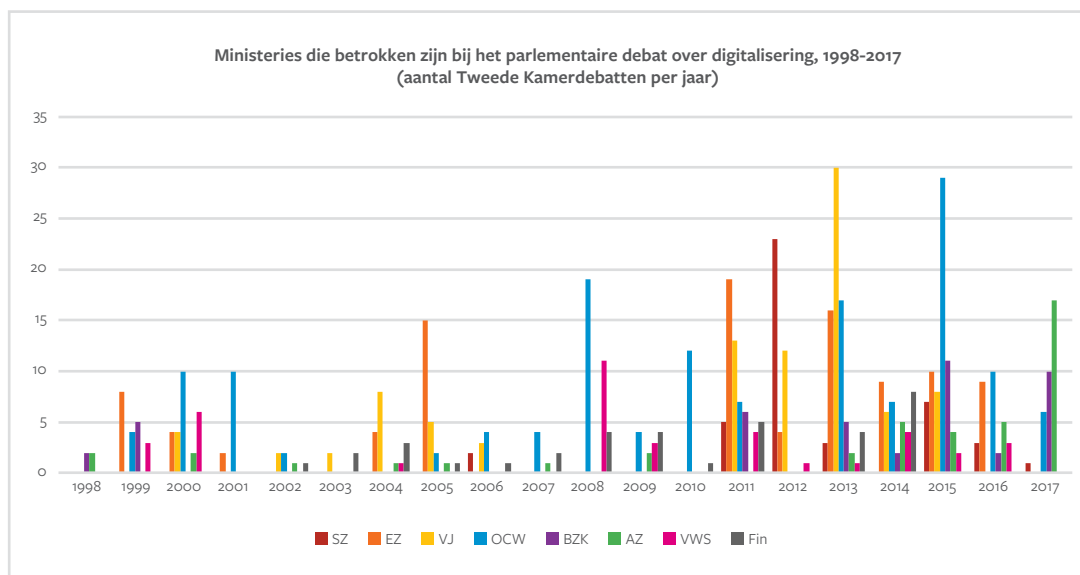


Voorts laten de woordwolken zien dat de Tweede Kamer stilstaat bij de technologische kant van het digitaliseringsvraagstuk. De encryptie van data, de kans om gehackt te worden, robotisering en blockchain-technologie zijn enkele onderwerpen waarover de Tweede Kamer heeft gedebatteerd.

Betrokkenheid van fracties, Tweede Kamerleden en bewindspersonen

Van significante verschillen tussen de fracties in de omvang van hun bijdragen aan het debat over digitalisering is geen sprake. De digitale analyse laat ook goed zien welke Tweede Kamerleden optraden als woordvoerders op dit terrein. Onder andere Verhoeven (D66), Segers (ChristenUnie), Oosenbrug (PvdA), Gesthuizen (SP) en haar partijgenoot Hijink behoren tot de Kamerleden die op dit terrein veelvuldig het woord hebben gevoerd. Zij treden in de voetsporen van Cherribi (VVD) en Wagenaar (PvdA), die in de jaren negentig als de eerste ICT-woordvoerders te boek stonden. Dat doorgaans een beperkt aantal Tweede Kamerleden zich mengt in het debat rond digitaliseringsvraagstukken, merken ook de Tweede Kamerleden zelf op.⁵ De kring van Tweede Kamerleden die zich in deze discussies mengt, is klein gebleven.⁶

De digitale analyse laat ook zien dat het aantal ministeries dat bij het debat over digitaliseringsvraagstukken betrokken is, in de loop van de tijd is uitgebreid. Aanvankelijk, rond 2004, voeren met name bewindspersonen van Justitie (Donner) en Economische Zaken (Brinkhorst) hierover het woord, later volgen ook collega's op het departement van Onderwijs (Plasterk en Van Bijsterveldt). Rond 2012 wordt het beeld diverser en treden met name de bewindspersonen op Binnenlandse Zaken – verantwoordelijk voor de bescherming van de grondrechten – nadrukkelijker naar voren, evenals de premier. Dat laatste gebeurt tegen de achtergrond van de introductie van een reeks digitale agenda's van de rijksoverheid. De toenemende betrokkenheid van de premier bij het thema laat zien dat de betekenis van digitalisering als politiek en maatschappelijk vraagstuk groeit.



Digitalisering: kwesties en crises

Hoewel een breed scala aan digitaliseringsthema's aan de orde is gekomen in het parlementaire debat, springen een aantal zaken eruit. In het begin van de onderzoeksperiode 2009-2019 is dat de DigiNotar-crisis uit juli 2011. Een bedrijf dat de beveiliging van Nederlandse overheidswebsites verzorgde, werd gehackt; het betekende de eerste cybercrisis waarmee de Nederlandse overheid werd geconfronteerd.⁷ Hoewel cybersecurity al voor deze hack op de agenda stond – in februari van dat jaar was de Nationale Cyber Security Strategie vastgesteld – nam de aandacht voor het thema toe in de nasleep van de DigiNotar-crisis.

In deze jaren is in de Tweede Kamer ook veel aandacht voor ICT-projecten bij de overheid, tegen de achtergrond van het parlementair onderzoek naar ICT-projecten bij de overheid dat een Tweede Kamercommissie (de commissie-Elias) tussen 2012 en 2014 uitvoert. De Tweede Kamer blijft vervolgens de uitvoering van ICT-projecten binnen de overheid kritisch volgen. Tegelijkertijd is de Tweede Kamer voorstander van een *open overheid*. In verschillende moties wordt de regering aangemoedigd een plan van aanpak rondom open data te ontwikkelen in dienst van transparante overheidscommunicatie.

Met name in de periode 2016-2019 speelt de Tweede Kamer een actieve rol in het agenderen van thema's op het gebied van digitalisering. Initiatiefnota's gaan onder meer over privacy, veilige apparaten, algoritmen en de positie van techgiganten.⁸ Ook neemt vanaf 2017-2018 het besef bij de Tweede Kamer toe dat digitalisering zich over meerdere beleidsterreinen uitstrekt, en afstemming tussen Tweede Kamercommissies daarom gewenst is. Van Dam (CDA) constateert dat digitalisering 'in allerlei commissies' speelt en roept de Tweede Kamer in april 2018 om op 'iets overkoepelends' te doen; ook andere Tweede Kamerleden geven aan behoefte hebben aan 'meer lijn'.⁹ De Tweede Kamer doet nog geen concrete voorstellen hoe dit gerealiseerd kan worden. Tegen deze achtergrond stelt de Tweede Kamer in 2019 de tijdelijke commissie Digitale toekomst in.

Met name de privacyaspecten van digitaliseringsvraagstukken staan op de radar van de Tweede Kamer; de verzameling van data en bijbehorende privacy-issues zijn haast met elk digitaliseringsdossier verbonden. De woordwolk op de pagina hiernaast maakt dit inzichtelijk.



De woordwolk laat zien dat digitaliseringsvraagstukken die met privacy worden geassocieerd onder meer raken aan het internet der dingen (apparaten) en digitale leermiddelen. De risico's die met digitalisering in verband worden gebracht hebben met name betrekking op hacken en het verspreiden van malware en hangen dus samen met cybersecurity.

Noten

- 1 *De Rijksbrede ICT-agenda. Beter presteren met ICT*, Handelingen van de Tweede Kamer der Staten-Generaal (HTK) 2003-2004 (1 maart 2004) Kamerstuk 26643, nr. 47; *ICT-Agenda 2008-2011. De gebruiker centraal in de digitale dienstenmaatschappij*, HTK 2007-2008 (13 juni 2008) Kamerstuk 26643, nr. 125.
- 2 Sociaal en Cultureel Planbureau, *In het zicht van de toekomst. Sociaal en Cultureel Rapport 2004* (Den Haag 2004) p. 17.
- 3 *Kamerbrief over Digitale agenda*, HTK 2015-2016 (5 juli 2016) Kamerstuk 29515, nr. 390. Overige bij de agenda betrokken ministeries zijn Binnenlandse Zaken en Koninkrijksrelaties; Volksgezondheid, Welzijn en Sport; Infrastructuur en Milieu; Onderwijs, Cultuur en Wetenschap en Veiligheid en Justitie.
- 4 Zie bijvoorbeeld verkiezingsprogramma's Tweede Kamer en Europees Parlement: GroenLinks, *GroenLinks. Verkiezingsprogramma 1994-1998* (1994); CDA, *Samenleven doe je niet alleen* (1998); VVD, *Investeren in uw toekomst* (1998); CDA, *Slagvaardig en samen* (2010); PvdA, *Iedereen telt mee. De kracht van Nederland* (2010); VVD, *Orde op zaken* (2010); D66, *Anders Ja* (2010); PvdA, *Een verbonden samenleving* (2017); SP, *#PakDeMacht* (2017); CDA, *Keuzes voor een beter Nederland* (2017); ChristenUnie, *Hoopvol Realistisch* (2017).
- 5 HTK 2017-2018 (4 oktober 2017) vergadernr. 8, item 11.
- 6 Zie bijvoorbeeld het Algemeen Overleg van de vaste commissie voor Binnenlandse Zaken. HTK 2018-2019 (31 oktober 2018) Kamerstuk 26643, nr. 579; en het overleg over e-health, Algemeen Overleg met twee Kamerleden en 25 bezorgde burgers. HTK 2016-2017 (15 februari 2017) Kamerstuk 27529, nr. 147, p. 3.
- 7 Mondelinge vraag n.a.v. bericht 'Rijk toch bezorgd over hack DigiNotar'. HTK 2010-2011 (6 september 2011) vergadernr. 102, item 7.

- 8 Het betreft de volgende initiatiefnota's: *Initiatiefnota van het lid Verhoeven: Het Internet der Dingen: maak apparaten veilig!*, HTK 2016-2017 (24 november 2016) Kamerstuk 34613, nr. 2; *Initiatiefnota van de leden Oosenbrug en Nijboer: De financiële sector en big data*, HTK 2016-2017 (29 november 2016) Kamerstuk 34616, nr. 2; *Initiatiefnota van het lid Koopmans: Onderlinge privacy*, HTK 2017-2018 (5 april 2018) Kamerstuk 34926, nr. 2; *Initiatiefnota van de leden Middendorp en Verhoeven: Online identiteit en regie op persoonsgegevens*, HTK 2017-2018 (6 september 2018) Kamerstuk 34993, nr. 2; *Initiatiefnota van het lid Verhoeven: Mededinging in de digitale economie*, HTK 2018-2019 (5 februari 2019) Kamerstuk 35134, nr. 2; *Initiatiefnota van het lid Middendorp: Menselijke grip op algoritmen*, HTK 2018-2019 (29 mei 2019) Kamerstuk 35212, nr. 2.
- 9 HTK 2017-2018 (12 april 2018) vergadernr. 73, item 6, p. 6.

Hoofdstuk 2

Vijf digitaliseringsvraagstukken nader onderzocht

Om verder inzicht te verkrijgen in de belangrijkste patronen in het parlementaire debat over digitalisering, zijn vijf casestudies onderworpen aan een nader kwalitatief onderzoek. Deze selectie van vijf casussen omvat digitaliseringsvraagstukken op sterk uiteenlopende beleidsterreinen, van onderwijs tot gezondheidszorg, vraagstukken die raken aan verschillende publieke waarden, van privacy tot machtsverhoudingen en die samen de gehele periode van onderzoek bestrijken.

De uiteenlopende reikwijdte stelt ons in staat om te onderzoeken in hoeverre de Tweede Kamer in het parlementaire debat over digitalisering verschillende accenten legt: meer of minder nadruk op kansen en risico's, en meer of minder aandacht voor publieke waarden. De verschillende aard van de casestudies maakt het ook mogelijk om in kaart te brengen hoe de Tweede Kamer zich verhoudt tot de overige partijen die bij digitaliseringsvraagstukken zijn betrokken – van het rijk en lokale overheden tot private en maatschappelijke organisaties.

In dit hoofdstuk leggen we kort uit welke casestudies we geselecteerd hebben. Bij elke casus lichten we toe in welke periode dit vraagstuk speelde, de ministeries die erbij betrokken waren, de publieke waarden die in het debat aan de orde werden gesteld en de maatschappelijke vraagstukken die ermee verband houden. Ook zetten we de vragen uiteen aan de hand waarvan het onderzoek is uitgevoerd. De meer uitgebreide analyses van de afzonderlijke casestudies zijn als bijlagen 1 tot en met 5 aan dit rapport toegevoegd.

Open data (2011 -)

PUBLIEKE WAARDEN	Transparantie, privacy, kansengelijkheid
MAATSCHAPPELIJKE VRAAGSTUKKEN	Toegankelijkheid van overheidsinformatie, gegevensbescherming
MINISTERIES	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Open data zijn digitale gegevens die vrij toegankelijk zijn en zonder beperkingen kunnen worden hergebruikt. Het gaat niet alleen om overheidsinformatie die digitaal beschikbaar is, maar juist ook om de onderliggende 'ruwe' data. Open data maken de overheid voor burgers transparanter en toegankelijker én stellen ondernemers in staat om nieuwe toepassingen te ontwikkelen. Tegelijkertijd roept het vragen op met betrekking tot de privacy van persoonsgegevens. Het onderwerp komt in 2011 op de agenda van de Tweede Kamer en krijgt met name tussen 2014 en 2016 veel aandacht. Bewindspersonen van Binnenlandse Zaken en Koninkrijksrelaties en Economische Zaken zijn bij het debat betrokken.

Cybersecurity (2011 -)

PUBLIEKE WAARDEN	Privacy, veiligheid, controle over techniek
MAATSCHAPPELIJKE VRAAGSTUKKEN	Veiligheid digitale communicatie tussen burger en overheid; desinformatie verkiezingen; burgerprivacy versus nationale veiligheid
MINISTERIES	Justitie en Veiligheid/Veiligheid en Justitie, Binnenlandse Zaken en Koninkrijksrelaties, Buitenlandse Zaken, Onderwijs, Cultuur & Wetenschap

De digitale analyse laat zien dat de hack bij DigiNotar in 2011 een belangrijk referentiekader vormt voor de Tweede Kamer in het debat over cybersecurity. Dat debat wordt met name tussen 2017 en 2019 gevoerd. Voor ons onderzoek is cybersecurity vooral relevant omdat het raakt aan publieke waarden als (nationale) veiligheid, privacy en controle over technologie. Bovendien kunnen we aan de hand van dit debat het krachtenveld rond digitaliseringsvraagstukken onderzoeken. Naast verschillende ministeries (Buitenlandse Zaken, Justitie en Veiligheid, Binnenlandse Zaken en Koninkrijksrelaties, Onderwijs, Cultuur en Wetenschap, betreft dit onder meer de internationale 'techreuzen', een organisatie als het National Cyber Security Centrum en samenwerking in EU-verband.

eHealth (2012 -)

PUBLIEKE WAARDEN	Privacy, veiligheid, controle over technologie, menselijke waardigheid
MAATSCHAPPELIJKE VRAAGSTUKKEN	Gegevensbescherming, mentale privacy, fysieke patiëntveiligheid, verantwoordelijkheid voor gebruik en opslag gegevens, controle over technologie, instrumentalisering en dehumanisatie van de zorg, toegankelijkheid van de zorg, werkloosheid
MINISTERIES	Volksgezondheid, Welzijn en Sport

In 2014 worden de doelstellingen van het ministerie voor Volksgezondheid, Welzijn en Sport (VWS) rondom eHealth van kracht. Deze gaan over drie onderwerpen: 1) online inzage in medische gegevens; 2) zelfmeten en gegevensmonitoring en 3) beeldschermzorg en domotica (het automatiseren van processen in huis, denk aan sensoren en camera's). Hierbij kunnen publieke waarden als privacy, veiligheid en menselijke waardigheid in het geding komen en die zijn ook deels in het debat aan de orde gesteld. De breedte van het thema eHealth spreekt uit de verschillende technologische toepassingen die in het debat voorbijkomen, zoals virtual reality (VR) en de ontwikkeling van het Elektronisch Patiëntendossier (epd) en de problemen die hierbij zijn ontstaan. Dit dossier had de Tweede Kamer al vroeg bewust gemaakt van het belang om gebruikers en hun behoeften te betrekken bij het ontwerp van een dergelijk systeem.

ICT in het onderwijs (2013 -)

PUBLIEKE WAARDEN	Privacy, kansgelijkheid
MAATSCHAPPELIJKE VRAAGSTUKKEN	Gegevensbescherming van leerlingen (pseudonimisering), kansen(on)gelijkheid in het onderwijs, digitale vaardigheid van leerling en docent
MINISTERIES	Ministerie van Onderwijs, Cultuur en Wetenschap, Ministerie van Economische Zaken

ICT in het onderwijs vormt de vijfde casus die in dit onderzoek is meegenomen. Naar aanleiding van een onderzoeksrapport van PricewaterhouseCoopers over de vraag hoe scholen en uitgeverijen omgaan met de privacy van leerlingen, voert de Tweede Kamer in 2015 een plenair debat met de bewindspersonen van Onderwijs, Cultuur en Wetenschap over privacy in het onderwijs, en de kansen en risico's die verbonden zijn aan digitalisering in het onderwijs. Dit resulteert uiteindelijk in de wijziging van diverse onderwijswetten. Zo komt onder meer een regeling tot stand om de persoonsgegevens van onderwijsdeelnemers te beschermen en beveiligen. Mede aan de hand van dit debat kan worden onderzocht hoe de Tweede Kamer eerder in het proces een afweging kan maken tussen de verschillende (democratische) waarden, kansen en risico's die met digitalisering zijn gemoeid.

SyRI (2014 -)

PUBLIEKE WAARDEN	Privacy, rechtvaardigheid, controle over techniek
MAATSCHAPPELIJKE VRAAGSTUKKEN	Gegevensbescherming, doelverschuiving technologie, surveillance, discriminatie, stigmatisering
MINISTERIES	Sociale Zaken en Werkgelegenheid, Veiligheid en Justitie/Justitie en Veiligheid, Economische Zaken

SyRI (Systeem Risico Indicatie) is een overheidssysteem om persoonsgegevens van burgers te koppelen en te analyseren. Het is vooral bedoeld om socialezekerheidsfraude te bestrijden. De ontwikkeling van SyRI hangt samen met verschillende digitaliseringstrends, zoals het gebruik van big data, algoritmes en artificial intelligence (AI). Het debat over het gebruik van dit systeem richt zich op democratische waarden als privacy en rechtvaardigheid. Met name de ministeries van Sociale Zaken en Justitie en Veiligheid zijn bij dit debat betrokken.

Analysekader

Voor elk van deze casestudies zijn zowel plenaire Tweede Kamerdebatten als commissievergaderingen onderzocht. Hierbij is gebruikgemaakt van een uitgebreid analysekader. Drie aspecten hebben bijzondere aandacht gekregen, omdat ze inzicht bieden in de inhoudelijke patronen in het debat en de institutioneel-strategische keuzes van de Tweede Kamer.

1. De informatiepositie van de Tweede Kamer en de ontwikkelingen die hierin zijn opgetreden

- Hoe laat de Tweede Kamer zich informeren, wat zijn de belangrijkste informatiebronnen?
- Naar welke informatie(bronnen) verwijst de Tweede Kamer in het debat?
- Hoe schat de Tweede Kamer de eigen informatiepositie in?

2. De rol die de Tweede Kamer speelt in het debat: informerend, agenderend en regulerend

- Wat vormt de aanleiding voor het debat?
- Welke instrumenten gebruikt de Tweede Kamer, zoals moties, amendementen, initiatiefwetgeving en initiatiefnota's?

3. De kansen, risico's en dilemma's in het Tweede Kamerdebat

- Hoe definieert de Tweede Kamer digitalisering(svraagstukken)?
- In hoeverre betreft de Tweede Kamer zowel kansen als risico's en maakt ze op basis hiervan een afweging?
- Met welke publieke waarden wordt digitalisering in het debat positief of negatief geassocieerd?

Hoofdstuk 3

De informatiepositie van de Tweede Kamer

Voor grip op digitaliseringsvraagstukken is een juiste, effectieve informatievoorziening cruciaal. In dit onderzoek hebben we ons afgevraagd welke partijen – politiek, bestuurlijk en maatschappelijk – bij het voorliggende vraagstuk zijn betrokken. Twee vragen zijn hieraan gerelateerd: heeft de Tweede Kamer deze stakeholders goed in beeld, met name de maatschappelijke partijen? En, vanuit het perspectief van informatie-input: door wie laat de Kamer zich informeren?

Ons onderzoek maakt duidelijk dat informatiegebrek niet de eerste zorg van de Tweede Kamer is. Met name op basis van rapporten van het Rathenau Instituut is de Tweede Kamer nieuwe onderwerpen gaan agenderen en meer aandacht gaan besteden aan publieke waarden. Ook andere kenniscentra, adviesorganen en belangenorganisaties weten de Kamer te bereiken. Tegelijkertijd wordt het voor de Kamer moeilijker om een integrale belangenafweging te maken, vanwege de omvang van de informatiestroom en de uiteenlopende perspectieven op digitaliseringsvraagstukken. Tegen deze achtergrond is de Tweede Kamer erbij gebaat om meer regie te hebben over hoe ze aan haar informatie komt, en van wie die komt. Ook heeft ze er baat bij om systematisch publieke waarden, kansen en risico's te betrekken bij het debat over digitalisering.

Informatiebronnen van de Tweede Kamer

De belangrijkste informatiebron van de Kamer is het kabinet. Via brieven en mondelinge toelichting in algemene overleggen rapporteren de verschillende bewindspersonen aan commissies en Kamer. Afgelopen jaren kreeg de Kamer meer en vaker agenda's en monitors aangeboden vanuit de rijksoverheid, adviesraden en kennisinstituten. Het overzicht van regeringsagenda's en onderzoeksrapporten, dat als bijlage bij dit rapport is opgenomen, geeft hiervan een goed beeld.

Een bijzondere rol is weggelegd voor het Rathenau Instituut, dat bijna 35 jaar geleden werd opgericht om onderzoek te doen naar sociaal-maatschappelijke gevolgen van de invoering van nieuwe technologieën (*technology assessments*). De afgelopen jaren heeft dit instituut grote invloed gehad op de richting en focus van het debat, met een reeks rapporten over publieke waarden die in het geding zijn bij digitale technologieën die zich razendsnel ontwikkelen (zie tabel \$\$\$). In februari 2017 publiceerde het RI het rapport *Opwaarderen*, als antwoord op de vraag van de Eerste Kamer aan het kabinet of de samenleving wel genoeg aandacht besteedde aan de ethische kant van digitalisering. De conclusie dat belangrijke publieke waarden onder druk staan, resoneert sindsdien in het parlementaire debat. Dat geldt ook voor de terminologie die het RI hierbij heeft aangereikt.

Publieke waarden en maatschappelijke vraagstukken die verbonden zijn aan digitalisering

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

Bron: Kool e.a., *Doelgericht digitaliseren* (2018) 14.

Zoals uit bovenstaande tabel blijkt, verbindt het Rathenau Instituut publieke waarden hoofdzakelijk aan risico's van digitalisering voor de samenleving en burgers. Is er bijvoorbeeld menselijke waardigheid in het geding, dan dreigen vooral gevaren voor de persoonlijke levenssfeer. Buiten beschouwing blijven hier de mogelijke positieve gevolgen van digitale toepassingen in termen van menselijke waardigheid, zoals bijvoorbeeld verbetering van persoonlijke vaardigheden of juist vergroting van werkgelegenheid. In veel gevallen betreft het twee zijdes van dezelfde medaille, van kans en risico. De Tweede Kamer lijkt daar in het ene vraagstuk beter oog voor te hebben dan in het andere. In het open datadebat is de Kamer zich zeer bewust van de kansen die digitalisering biedt voor de bevordering van publieke waarden als transparantie en burgerbetrokkenheid; de fraudeopsporing met behulp van SyRI was onder meer ingegeven door de kans op vergroting van maatschappelijk draagvlak voor het sociaal zekerheidsstelsel.

Ook de digitale technologieën waarvoor de Tweede Kamer volgens het RI enigszins een blinde vlek leek te hebben ontwikkeld, worden inmiddels vaker aangekaart. Denk bijvoorbeeld aan de maatschappelijke impact van algoritmegebruik en, recenter, de manier waarop AI-toepassingen ingrijpen in de fysieke wereld en het leven van mensen. Terwijl VR-technologie over het algemeen nog weinig politieke aandacht trekt, agendeert de Kamer het in 2015-2016 bij een debat over het gebruik van 'serious games' in de zorg.¹ Als het gaat om de – uitzonderlijk snelle – ontwikkelingen op het gebied van digitalisering, is enigszins achter de feiten aanlopen niet te voorkomen, maar de Kamer houdt in de hier onderzochte dossiers aardig de vinger aan de pols.

Naast het Rathenau Instituut weten ook andere kenniscentra de Tweede Kamer goed te bereiken. Nictiz, het Nationaal ICT Instituut in de Zorg, presenteert jaarlijks een eHealth-monitor, er is een Nationale Open Data Agenda en de Cyber Security Raad draagt bij aan de Nationale Cybersecurity Agenda die de regering heeft vastgesteld. Daarnaast zijn er rapporten van allerlei onderzoeksinstituten die zich gebogen hebben over digitalisering in uiteenlopende terreinen van de samenleving.

In het parlementaire debat over digitalisering is goed te zien dat het Nederlandse adviesstelsel sterk is ontwikkeld. Zeker op het terrein van zorg (Raad voor Volksgezondheid) en onderwijs (onder meer PO- en VO-raad) hebben de adviesraden afgelopen jaren een belangrijke rol gespeeld in het signaleren en concretiseren van de kansen en risico's van digitalisering binnen de eigen sector. Zo droeg een verkennend advies van de Raad voor Volksgezondheid (begin 2019) over de kansen en risico's van kunstmatige intelligentie in de zorg er bijvoorbeeld toe bij dat in het debat over eHealth nu meer aandacht is voor de maatschappelijke keerzijdes ervan, na een jarenlange focus op de voordelen van betere en meer doeltreffende zorg-op-maat.² Ook op andere beleidsterreinen roepen kabinet en Kamer regelmatig hulp in, of krijgen ze ongevraagd advies, van adviesraden als de Raad van State,

de Wetenschappelijke Raad voor het Regeringsbeleid (WWR), het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) en de Raad voor het Openbaar Bestuur (ROB).

Analyse van het parlementaire debat maakt eveneens goed zichtbaar welke beleidsterreinen een sterk georganiseerd en geïnstitutionaliseerd netwerk van belangenorganisaties kennen. Naast de 'klassieke' NGO's over mensenrechten zijn er inmiddels talrijke maatschappelijke organisaties die zich bezighouden met de maatschappelijke gevolgen van digitalisering, of aspecten daarvan. Ook zij weten hun weg naar de Tweede Kamer te vinden en invloed uit te oefenen. De *Open State Foundation* heeft afgelopen jaren de kar getrokken in een actieve en succesvolle lobby van diverse maatschappelijke organisaties voor digitale transparantie. Rond privacy is een uitgebreide coalitie van platforms en belangenorganisaties ontstaan, die met duidelijke steun van de media ook de Tweede Kamer weten te bereiken, van Privacy First tot het Platform Bescherming Burgerrechten.

De input van dit soort organisaties heeft ertoe bijgedragen dat de Kamer digitaliseringsvraagstukken vanuit (meer) verschillende invalshoeken is gaan bezien. De keerzijde is dat het debat hierdoor diffuser is geworden en soms ook meer eenzijdig. De SyRI-casus laat bijvoorbeeld zien dat de oorspronkelijke doelstellingen van het systeem – fraudeopsporing met name – naar de achtergrond verdwijnen, vanaf het moment dat privacy als vraagstuk in het debat wordt gebracht.

Aangereikte informatie versus eigen informatiebehoefte

Aan informatie ontbreekt het de Kamer kortom niet. Toch wordt het gevoel van 'grip' daar niet per se groter door. De integrale belangenafweging wordt moeilijker door de omvang van de informatiestroom die op de Kamer afkomt, de soms technologisch complexe materie en de veelheid aan aspecten die in rapporten en monitors wordt belicht, terwijl zulke documenten niet altijd onderlinge verbanden tussen vraagstukken benoemen. De indruk is dat overvloed aan informatie op dit moment een groter probleem voor de Kamer is dan gebrek aan informatie.³

De spanning tussen te veel en te weinig informatie doet zich met name voor in technologisch complexe of veelomvattende dossiers, zoals open data en eHealth. Hier heeft toevloed aan informatie en het inwinnen van expertise geleid tot een nadruk op specifieke technologische (toepassings)vraagstukken.

Een ander risico is dat de Tweede Kamer zelf nog maar beperkt regie voert over van wie zij welke informatie krijgt. Hoe overvloediger de informatiestroom, hoe moeilijker het bovendien is om te bepalen waar de eigen informatiebehoefte ligt, gelet op de bredere vraag naar de maatschappelijke impact van digitale ontwikkelingen. De Tweede Kamer lijkt haar handen vaak al meer dan vol te hebben aan de verwerking van aangeboden en beschikbare informatie. In een ideale situatie is de Tweede Kamer minder aanbodaafhankelijk in haar informatiegebruik en stelt ze gerichte informatievragen. Welke publieke problemen, belangen en belanghebbenden hebben wij nog niet in het vizier, of zijn nog niet in dit debat betrokken, maar zouden dat wel moeten zijn? Het meer systematisch uitvoeren van stakeholdersanalyses kan een manier zijn om per vraagstuk in de volle breedte belanghebbenden te identificeren, van burger tot bedrijfsleven en van media tot maatschappelijke organisaties. Ambtelijke ondersteuning speelt hierbij uiteraard een belangrijke rol, zowel bij het uitvoeren van zulke stakeholderanalyses als bij het snel(ler) mobiliseren en inzetten van relevante kennisnetwerken.

Regie over het inwinnen van informatie betekent ook dat de Kamer zich een afgewogen beeld vormt van de politieke en publieke dimensie van digitaliseringsvraagstukken. Dat betekent allereerst het benoemen van publieke waarden die in het geding komen door digitalisering. Het Rathenau Instituut brengt in zijn rapport *Doelgericht digitaliseren* (2018) een aantal belangrijke publieke waarden in kaart.

In het verlengde hiervan is het van belang om zowel risico's als kansen voor economie, overheid en samenleving mee te nemen en af te wegen. In het beoordelingskader (hoofdstuk 6) noemen wij een aantal hiervan.

Wat te midden van deze overvloed aan informatie ten slotte opvalt, is dat de Tweede Kamer beperkt gebruikmaakt van haar eigen geheugen, eerder gemaakte afwegingen en gevoerde debatten. Kamerleden betrekken debatten uit het recente verleden niet systematisch bij de discussie over vergelijkbare vraagstukken in het heden. De onderwijscasus laat bijvoorbeeld zien dat eerdere discussies in de Kamer over digitale leermiddelen (in de periode 2007-2008) tien jaar later niet worden meegenomen in het debat. Het is uiteraard niet zo dat het verleden per definitie richtinggevend moet zijn, maar meer inzicht in het handelen en de positiebepaling in het verleden, in de discussiepunten en eerder geformuleerde oplossingen kan de Tweede Kamer wel houvast bieden voor de oriëntatie op vergelijkbare vraagstukken in het heden.

Noten

- 1 D. Snijders e.a., *Verantwoord virtueel. Bescherm consumenten in virtual reality* (Den Haag 2019) 4; HTK 2015-2016 (27 januari 2016) vergadernr. 47, item 3, p. 7 en 14; HTK 2015-2016 (4 november 2015) vergadernr. 20, item 3, p. 14.
- 2 Raad van State, *Waarde(n)volle zorgtechnologie. Een verkennend advies over de kansen en risico's van kunstmatige intelligentie in de zorg* (Den Haag 2019).
- 3 De studie van Guido Enthoven, *Hoe vertellen we het de Kamer? Een empirisch onderzoek naar de informatierelatie tussen regering en parlement* (Utrecht 2011) p. 80-81, laat zien dat dit een breder gesignaleerd probleem is.

Hoofdstuk 4

De informerende, agenderende en regulerende rol van de Tweede Kamer

In dit hoofdstuk bespreken we hoe de Tweede Kamer de laatste jaren heeft opgetreden in het proces van beleids- en besluitvorming ten aanzien van digitalisering, welke rol zij hierin voor zichzelf zag weggelegd en waar ze haar prioriteiten heeft gelegd. In de parlementaire praktijk, zo laat ook onze analyse zien, zijn de formele rollen van de Tweede Kamer (controlerend, wetgevend en/of volksvertegenwoordigend) moeilijk te scheiden. Op basis van onze analyse constateren wij dat bij digitalisering drie houdingen de overhand hebben. In de eerste plaats heeft de Kamer aangedrongen op *versterking van haar kennis- en informatiepositie* – zowel bij de regering als bij zichzelf, door zelfstandig informatieverzoeken uit te zetten en onderzoek te laten doen. In de tweede plaats is de Tweede Kamer actiever geworden in het *agenderen* van digitaliseringsvraagstukken. In de derde plaats oriënteert de Kamer zich op mogelijkheden om de toepassing van digitale technologie *bij te sturen* via concrete beleidsmaatregelen en wetgeving.

De Tweede Kamer heeft digitalisering inmiddels duidelijk in het vizier. De agenderende rol overheerst, en dat verklaart ook het verlangen van de Kamer naar een meer overkoepelend of integraal overzicht over digitaliseringsvraagstukken. Daarnaast valt op dat de Kamer nadruk legt op publieke waarden, maar nog wel zoekende is in de manier waarop ze vorm moet geven een waardengedreven benadering. Deze zoektocht wordt niet vergemakkelijkt door het karakter van het podium waarop de meeste debatten worden gevoerd. In de commissievergaderingen, waarin doorgaans meer nadruk ligt op details van beleid en de techniek van ontwikkelingen binnen een specifiek domein, blijkt het soms lastig om een overkoepelende visie te ontwikkelen. Ook vindt het debat verspreid over verschillende commissies plaats.

Ten slotte heeft de Kamer te maken met een debat op twee niveaus. Enerzijds zijn er digitaliseringsvraagstukken die spelen binnen het overheidsapparaat. Hierover kan een Kamermeerderheid met de regering concrete afspraken maken. Anderzijds zijn er digitaliseringsvraagstukken waarbij marktpartijen zijn betrokken. Die laatsten opereren vaak op globale schaal – denk aan Huawei, Google of Facebook. Bij deze vraagstukken moeten Tweede Kamer en regering vooral kaderstellend denken en handelen, vanuit de publieke waarden die zij hoog willen houden.

Laten informeren

In het vorige hoofdstuk constateerden we dat de toevloed van informatie – in de vorm van beleidsvoorbereidende rapporten en adviezen – de Tweede Kamer eerder doet verlangen naar *overkoepelend overzicht* en *interpretatie* van informatie, dan naar *meer* informatie. De instelling van twee tijdelijke commissies toont dat de Tweede Kamer daar stappen in heeft gezet. De instelling van de tijdelijke commissie Digitale toekomst in 2019 is een logische vervolgstap van de Tweede Kamer om zich te oriënteren op digitaliseringsprocessen in heden, verleden en toekomst. Het is de tweede onderzoekscommissie in vijf jaar tijd op dit thema: tussen 2012 en 2014 verrichtte de tijdelijke commissie ICT-projecten bij de overheid uitgebreid onderzoek naar de besturing en beheersing van ICT-investeringen bij de rijksoverheid.

De vaste Kamercommissies spelen een centrale en coördinerende rol in de vergaring van informatie. Kamerbrieven en regelmatige algemene overleggen met bewindspersonen zorgen voor kennisopbouw en zijn een manier om de vinger aan de pols te houden. Rondetafelgesprekken zijn een gewaardeerd instrument om relatief snel en eenvoudig te horen hoe verschillende experts en stakeholders denken over een onderwerp. Omdat veel digitale innovaties zich echter over verschillende sectoren uitstrekken en op elkaar inwerken, signaleren Kamerleden dat de ‘verkokering’ van de parlementaire controle hier extra problematisch is.¹ Er is inmiddels geen beleidsterrein meer waarop digitalisering *geen* rol van betekenis speelt – ook al worden Economische Zaken, Binnenlandse Zaken, en Justitie en Veiligheid nog vaak aangewezen als de ministeries en vaste Kamercommissies die er het meest mee te maken hebben. Het instrumentgebruik van leden en fracties versterkt het beeld dat de Tweede Kamer vooral een integraal overzicht wil verkrijgen en kennis wil opbouwen op het gebied van digitalisering. Dat doet ze via concrete informatieverzoeken en schriftelijke vragen.²

Ook in de Eerste Kamer is de behoefte naar overzicht over digitaliseringstrends, en hun gevolgen voor de Nederlandse samenleving, gegroeid. Het was de Eerste Kamer die in september 2014 de regering per motie opriep om het Rathenau Instituut onderzoek te laten doen naar ‘de ethische kant’ van digitale toepassingen. Vanuit dit speerpunt laat ook de Eerste Kamer zich met enige regelmaat informeren over digitaliseringsprocessen, in het bijzonder bij de rijksoverheid, zowel in gedachtewisselingen met de regering als via gesprekken met externe deskundigen.³ De indruk is dat, voor zover er strategische afstemming tussen Tweede Kamerleden en senatoren plaatsvindt, deze via de eigen fractie verloopt.

Agenderen

Om invulling te geven aan haar taken, heeft de Tweede Kamer verschillende rechten. Tot de klassieke rechten behoren het vragen- en inlichtingenrecht, het recht van interpellatie, het recht van amendement en het recht van initiatief. Minder vaak genoemd, maar eveneens een belangrijk recht van de Kamer is de bevoegdheid om zelf de agenda van het parlementaire debat vast te stellen: om hierdoor kwesties van algemeen belang aan te kaarten en het politiek-maatschappelijke debat hierover aan te jagen. Door maatschappelijke zorgen te agenderen, geeft de Tweede Kamer uitdrukking aan haar volksvertegenwoordigende rol.

De laatste vijf jaar is de Kamer digitaliseringsvraagstukken meer gaan agenderen. Tot dan toe debatteerde het parlement vooral over digitalisering als het kabinet daartoe aanleiding af; bij begrotingsbehandelingen, behandeling van wetsvoorstellen en bij de bespreking van kabinetsbrieven en anderszins gepresenteerde informatie. De Tweede Kamer heeft hier een meer agenderende rol naar zich toegetrokken. Dat kan klein beginnen, bijvoorbeeld met een schriftelijke of mondelinge vraag naar aanleiding van een alarmerend nieuwsbericht. Het kan ook groot en breed worden ingestoken, met een initiatiefwetsvoorstel of instelling van een commissie. Daar tussenin liggen onder meer de aanvraag van een plenair speeddebat, het uitnodigen van de regering voor een algemeen overleg in commissieverband, of de indiening van moties om de Tweede Kamer zich te laten uitspreken over het belang van een bepaald vraagstuk.

RECENTE INITIATIEFNOTA'S OP HET GEBIED VAN DIGITALISERING (2016-2019)

- Het Internet der Dingen. Maak apparaten veilig (2016, Verhoeven, D66)
- Financiële sector en big data (2016, Oosenbrug en Nijboer, PvdA)
- Online identiteit en regie op persoonsgegevens (2018, Middendorp en Verhoeven, VVD/D66)
- Onderlinge privacy (2018, Koopmans, VVD)
- Menselijke grip op algoritmen (2019, Middendorp, VVD)
- Mededinging in de digitale economie. Data, techgiganten en vrije mededinging in een vrije economie (2019, Verhoeven, D66)

Enkele individuele leden zijn opvallend actief gebleken in het agenderen van digitaliseringsvraagstukken door middel van initiatiefnota's. De afgelopen vier jaar zijn, met uitzondering van verkiezingsjaar 2017, jaarlijks twee initiatiefnota's verschenen over digitalisering (op een totaal van gemiddeld vijftien nota's per jaar). Het is tekenend dat in deze initiatiefnota's, net als in de onderzoeksvraag van de Eerste Kamer uit 2014, bijzondere aandacht wordt gevraagd voor de gevolgen van digitale innovatie voor publieke waarden als veiligheid, privacy en controle van de mens over technologie. Vrijwel alle initiatiefnota's roepen regering en parlement op om meer oog te hebben voor risico's, maar tegelijkertijd kansen niet onbenut te laten.

Een veel sneller en daarom geliefd middel om kwesties te agenderen – en zich daarover nader te laten informeren – is het stellen van Kamervragen. Of in de Tweede Kamer verhoudingsgewijs veel vragen gesteld worden over digitalisering, zou nader onderzoek moeten uitwijzen. Het overzicht over de periode januari 2017-juni 2018 dat eerder door het Rathenau Instituut is samengesteld, laat in elk geval geen opvallend stijgende lijn zien. Inhoudelijk blijkt wel dat de meeste vragen zich richtten op incidenten van privacyschending, vaak naar aanleiding van berichtgeving in de pers. Het SyRI-dossier duikt in Kamervragen op, net als Cambridge Analytica en overtreding van de privacyregels door Facebook. In het algemeen lijkt privacy op dit moment de publieke waarde die de meeste aandacht van de Kamer krijgt. Menselijke waardigheid en rechtvaardigheid blijken in concrete Kamervragen moeilijker te hanteren waarden. Dat heeft ook met de aard van het instrument te maken; Kamervragen zijn al decennialang vooral geliefd als megafoon om de aandacht te vestigen op zorgelijke incidenten en ontwikkelingen – en op de verontwaardiging van de vragensteller daarover.

Minstens zo populair, ook in het parlementaire debat over digitalisering, is het formuleren van moties. De wens tot agendering en beïnvloeding gaan hier vaak hand in hand. Bezien we de voornaamste, breed gedragen moties van de afgelopen vijf jaar, dan valt echter vooral de relatief bescheiden opstelling van de Kamer op. De motieteksten weerspiegelen het verlangen naar 'grip', maar meer in de zin van 'bijbenen' dan 'bijsturen' van de ontwikkelingen op het terrein van digitalisering. Kenmerkend in dit verband zijn ook de moties waarin de Kamer oproept tot een duidelijke focus in het parlementaire debat over deze ontwikkelingen. Meest in het oog springt dan de motie van de Kamerleden Van Dam en Van der Molen (beiden CDA) van 6 juni 2018, waarin zij de regering oproepen om een 'waardengedreven benadering' te ontwikkelen ten aanzien van digitalisering en bij deze ontwikkeling ook de Kamer te betrekken. De minister voor Rechtsbescherming neemt deze motie over.⁴

Ook in de meer concrete oproepen tot actie aan het adres van de regering valt een zekere terughoudendheid te bespeuren. Verzoeken om actieplannen, doelstellingen, onderzoeken en overzichten lijken de overhand te hebben op moties waarin de Kamer zelf een duidelijke beleidsrichting aanwijst of oproept tot regulering. Op het terrein van eHealth werd de regering bijvoorbeeld opgeroepen een centraal digitaal punt in te richten, dat een overzicht biedt van goed werkende zorgapps. Op het terrein van cybersecurity werd de regering in een motie van Verhoeven en Middendorp (D66/VVD, 13 maart 2019) verzocht om een actieplan tegen digitale inmenging te formuleren ter bescherming van de democratische rechtsstaat.²

Reguleren

Concrete voorstellen vanuit de Tweede Kamer tot regulering ten aanzien van digitalisering zijn dan ook relatief schaars. Een eerste belangrijke uitzondering vormen de voorstellen die voortvloeien uit de hierboven genoemde initiatiefnota's. Een tweede belangrijke uitzondering ligt op het terrein van open data. In 2012 initieert Kamerlid Mariko Peters (GL) nieuwe wetgeving, en wel in de vorm van de Wet open overheid. Nadat Peters niet lang daarna de Kamer verlaten heeft, nemen collega-Kamerleden het voorstel over. Ook in dit dossier hangt de activiteit die de Kamer ontplooit op het terrein van digitalisering samen met de koppeling aan publieke waarden – in dit geval met name transparantie en een dienstverlenende overheid – én aan economische groei. De overheidsdata kunnen immers voor commerciële doeleinden hergebruikt worden en dat kan 'honderden miljoenen' opleveren voor de Nederlandse economie.⁵ Het wetsvoorstel zal naar verwachting het komende jaar terugkeren op de parlementaire agenda. Een tweede initiatiefwetsvoorstel is onlangs aangekondigd en gaat over de introductie van een wettelijk afwegingskader voor cyberwapens.⁶

Het oppakken van een regulerende rol op het gebied van digitalisering blijkt lastig. Dat komt door de snelle technologische ontwikkelingen en de globale schaal waarop deze zich voltrekken; wetgeving kan al snel verouderd zijn en het is lastig grip krijgen op globaal opererende 'techreuzen' als Google en Facebook. De remedie hiervoor is – deels – 'technologieneutraal' of 'technologieonafhankelijk' wetgeven. Onder meer in het kader van aanpassing van artikel 13 van de Grondwet (brief- en telecommunicatiegeheim) heeft de Kamer hierover gedebatteerd.⁷ Ook aan deze vorm van wetgeving zitten echter haken en ogen, zoals de Raad van State in een advies uit 2018 heeft uiteengezet.⁸

Noten

- 1 HTK 2017-2018 (12 april 2018) vergadernr. 73, item 6.
- 2 Overzicht op basis van eigen analyse voor de periode juni 2018-december 2019, vergeleken met de peiling van januari 2017-juni 2018 door het Rathenau Instituut. Kool e.a, *Doelgericht digitaliseren*, p. 151-159.
- 3 Kool e.a, *Doelgericht digitaliseren*, p. 90.
- 4 Overzicht op basis van eigen analyse van aangenomen Kamermoties gericht op digitaliseringsprocessen in de periode juni 2018-december 2019, vergeleken met de peiling van januari 2017-juni 2018 door het Rathenau Instituut. Kool e.a, *Doelgericht digitaliseren*, p. 151-159; HTK 2017-2018 (6 juni 2018) vergadernr. 90, item 3, p. 5.
- 5 HTK 2015-2016 (8 december 2015) Kamerstuk 32802, nr. 22, p. 2.
- 6 Kees Verhoeven, *Techvisie 2.0* (2019), raadpleegbaar via <<http://www.d66.nl>>
- 7 HTK 2016-2017 (12 april 2017) vergadernr. 67, item 3.
- 8 Raad van State, *Ongevraagd advies over de effecten van de digitalisering voor de rechtsstatelijke verhoudingen*. HTK 2017-2018 (5 september 2018) Kamerstuk 26643, nr. 557.

Hoofdstuk 5

Argumentatiepatronen in het parlementaire debat

In dit hoofdstuk analyseren we hoe de Tweede Kamer digitalisering en digitaliseringsvraagstukken heeft gedefinieerd. We bespreken daarnaast in hoeverre de Tweede Kamer in het parlementaire debat over digitalisering zowel kansen als risico's heeft betrokken en met welke publieke waarden zij digitalisering positief of negatief geassocieerd heeft.

De analyse van de vijf uitgekozen digitaliseringsvraagstukken laat zien dat de meeste debatten beginnen vanuit de kansen en voordelen van bepaalde digitale toepassingen. Na verloop van tijd verschuift de discussie in de Tweede Kamer echter naar de risico's die hiermee gemoeid zijn en de publieke waarden die daaraan raken, vaak ook onder invloed van het publieke debat. De kansen verdwijnen dan naar de achtergrond. In beide gevallen wordt het debat vooral vanuit één perspectief gevoerd.

Tegelijkertijd laat onze analyse zien dat de Tweede Kamer aan houvast en daadkracht wint, wanneer het debat vanuit het streven naar waarborging van publieke waarden wordt gevoerd en digitalisering in de eerste plaats als publiek en politiek vraagstuk wordt benaderd. Hoewel de Kamer overvallen werd door de ontwikkelingen binnen het SyRI-dossier, leverden de discussies over algoritmes wel een heldere politisering van digitalisering op. Er ontstond een fundamenteel debat over de vraag hoe digitalisering zich verhoudt tot publieke waarden als privacy, rechtvaardigheid en menselijke controle over technologie.

Veel recente initiatiefnota's op het terrein van digitalisering zijn eveneens ingegeven door de bescherming van publieke waarden. Ook het open data-dossier laat de relatie tussen publieke waarden en houvast zien. De druk op de minister vloeit voort uit het geloof van de Tweede Kamer in de kansen die digitalisering biedt voor een nieuwe, open verhouding tussen overheid en burger; een transparante overheid, die data beschikbaar stelt en zo burgers meer inzicht biedt in beleid. Verschillende Kamerleden spreken over de 'cultuuromslag' en 'cultuurverandering' die op dit terrein nodig is onder bestuurders en ambtenaren, te beginnen op de ministeries.¹

Een definitie van digitalisering

Uit de analyse van de casestudies rijzen drie benaderingen van digitalisering op. Op de eerste plaats verwijst digitalisering naar het in gebruik nemen van digitale middelen en instrumenten. Dat komt neer op een benadering van digitalisering als ICT. Denk aan digitale communicatie tussen overheid en burger, het gebruik van digitale leermiddelen in het onderwijs of de beveiliging van de digitale infrastructuur. Op de tweede plaats verwijst digitalisering naar een proces, een ontwikkeling die onze samenleving beïnvloedt, waarbij tal van publieke waarden in het geding zijn. In deze definitie omvat digitalisering het geheel van verzameling, analyse en toepassing van informatie afkomstig uit digitale middelen. Ten derde, en dit laten vooral de onderwijs- en eHealth-casus goed zien, verwijst digitalisering naar de digitaal vaardig wordende mens; het in staat zijn van burgers om te functioneren in een steeds sterker gedigitaliseerde samenleving en effectief en productief gebruik te maken van digitale middelen.

Waarden, kansen, risico's

De analyse van de casestudies laat in combinatie met de digitale analyse de verschillende invalshoeken zien van waaruit het debat over digitalisering in de Kamer wordt gevoerd; we duiden die hier aan als argumentaties ten aanzien van digitalisering. Het wekt geen verbazing dat digitalisering op het gebied van Economische Zaken wordt besproken vanuit de kansen die het biedt voor economische groei, terwijl bij Justitie logischerwijs rechtsbescherming en veiligheid de dominante invalshoek vormen. Onderwijs en Volksgezondheid nemen hier een aparte positie in. Terwijl voor de meeste beleidsterreinen digitalisering een middel tot een doel is, presenteren deze twee beleidsterreinen digitalisering als doel op zich: via het onderwijs kan de samenleving 'digivaardig' worden gemaakt en kunnen (jonge) burgers toegerust worden voor een leven in de digitale samenleving. Deze digitale vaardigheid wordt niet louter praktisch ingevuld, maar omvat ook bewustwording van de kansen en risico's die met digitalisering verbonden zijn. De Kamer heeft hierbij oog gehad voor de publieke waarden van rechtvaardigheid en inclusie; de taak van de overheid om ertoe bij te dragen dat álle burgers meekomen in de digitale transformatie, waarbij met name de oudere generatie aandacht heeft gekregen.

Een ander kenmerk van de argumentaties in het parlementaire debat over digitalisering is de nadruk op het technologische aspect. Technologische vernieuwing vormt een belangrijk onderdeel van de beleidsontwikkeling op het gebied van digitalisering in de publieke sector, met de bijbehorende financiële investeringen in digitale infrastructuur en technieken. De complexiteit van de technologie en de hoge ontwikkelsnelheid dragen bij aan het gevoel van de Tweede Kamer geen grip te hebben. Kamerleden geven ook in debatten aan de voorliggende materie ingewikkeld – 'vreselijk technisch' – te vinden en typeren thema's als algoritmes als 'uitermate lastig ... om daar nou eens even helder over te communiceren.'² Staatssecretaris Knops (BZK) merkte in 2018 tijdens een algemeen overleg over open data echter op dat politici 'niet per se de techniek tot in de finesses' moeten beheersen, maar vooral tot taak hebben 'te begrijpen wat de maatschappelijke impact is'. Het doordenken van kansen en risico's vanuit publieke waarden kan het begrip voor de maatschappelijke impact van digitalisering versterken.

Ontwikkelingen in de argumentatiepatronen vanaf 2014

Hoewel de Tweede Kamer al vanaf de tweede helft van de jaren negentig oog heeft gehad voor de risico's of schaduwzijden van digitalisering, voert het denken in termen van kansen aanvankelijk de boventoon. Digitalisering brengt de overheid dichterbij de burger, maakt zorg toegankelijker, maakt het mogelijk om fraude effectiever op te sporen en stimuleert niet in de laatste plaats economie en innovatie. Tot en met 2018 vallen debatten over eHealth onder de noemer 'innovatie'. De Kamer legt in dit dossier aanvankelijk de nadruk op de consumptieve kant en verbetering van de kwaliteit van leven; eHealth biedt kansen om zorg voor patiënten op afstand beschikbaar te stellen en de patiënt kan zelf zijn zorgbehoefte beter inschatten. Ook het economische argument van kostenbesparing komt voorbij. In het geval van cybersecurity en open data komt later eveneens meer oog voor de risico's, met name op het gebied van privacy en de ongewenste effecten van de vermarkting van open data.

In vrijwel alle digitaliseringsvraagstukken treedt na verloop van tijd een soortgelijke verschuiving op, waarbij naast kansen ook risico's in beeld komen. Over het algemeen geldt dat het privacyvraagstuk als eerste de aandacht van de Kamer heeft, bijvoorbeeld als het gaat over de omgang met leerlinggegevens of medische gegevens in het Elektronisch Patiëntendossier. Gaandeweg komen meer waarden in het vizier.

Een tweede verschuiving die zich door de tijd aftekent, is nauw verbonden met deze toenemende aandacht voor risico's. De benadering waarin technologische innovatie op zichzelf centraal stelt maakt plaats voor een benadering waarbij de Tweede Kamer digitalisering meer gaat zien als een ontwikkeling in

dienst van de mens. Technologie wordt een hulpmiddel om te voldoen aan wensen en behoeften vanuit overheid en samenleving. In het eHealth-dossier is dit bijvoorbeeld terug te zien in de steun vanuit de Kamer in 2016 voor een wetsvoorstel voor de bekostiging van anonieme e-mentalhealth. De Kamer omschrijft dat als een mooi voorbeeld 'van het organiseren van zorg vanuit de vraag en de wensen van mensen in plaats van op basis van het denken vanuit een systeem.'³

In elk van de onderzochte casussen valt wel een keerpunt aan te wijzen – in het ene geval preciezer dan het andere – waarop de Kamer een bredere blik op het vraagstuk ontwikkelt, impliciet of expliciet. Zo komt in het onderwijsdebat in 2017 vanuit de Kamer een oproep om een 'breder debat' te voeren 'over de kansen en risico's van digitalisering'.⁴ Hoe dit concreet moet worden aangepakt en wat uitgangspunt en doel van zo'n debat zouden moeten zijn, maakt de Tweede Kamer nog niet duidelijk. In de SyRI-casus vormt een incident – ambtenaren zoeken persoonlijke gegevens van Bekende Nederlanders op – aanleiding voor de Kamer om invulling te geven aan haar volksvertegenwoordigende rol. Ze stelt de regering vragen over de bescherming van persoonsgegevens en het gebruik van algoritmes bij fraudeopsporing. Waarden als democratische machtsverhoudingen en rechtvaardigheid vormen de achtergrond waartegen de Kamer het onterecht uitdelen van boetes aan de orde stelt.

Kortom: een waardengerichte benadering is in opkomst. Van de Tweede Kamer vraagt dat een nadere doordenking van hoe de discussie over waarborging van publieke waarden uiteindelijk kan leiden tot concrete voorstellen voor beleidsmaatregelen en wetgeving. Onze analyse laat in elk geval zien dat het debat effectief gevoerd kan worden zonder dat méér technologische (dossier)kennis vereist is. De Tweede Kamer heeft vooral behoefte aan een integrale belangenafweging van kansen en risico's van digitalisering. Een beoordelingskader dat helpt om die afweging te maken, kan daarbij een belangrijk hulpmiddel zijn. In het volgende hoofdstuk introduceren we zo'n kader.

Noten

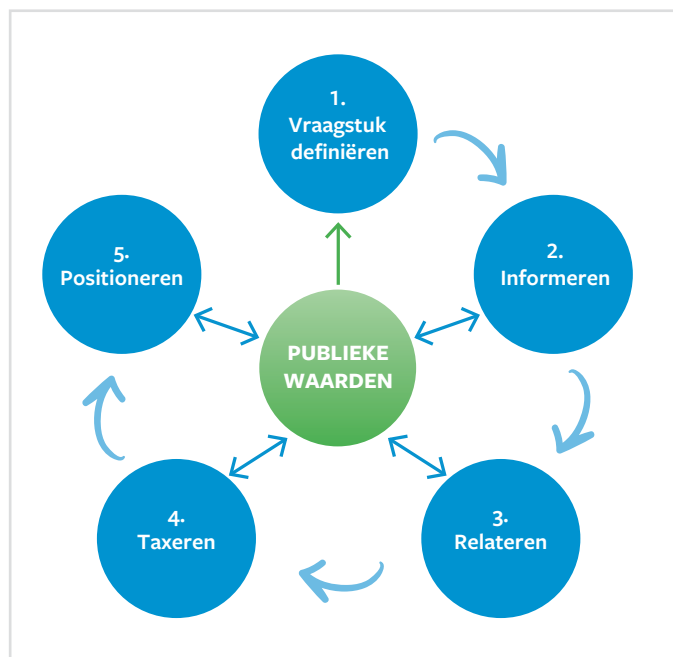
- 1 HTK 2016-2017 (7 september 2016) Kamerstuk 32802, nr. 30, p.3.
- 2 HTK 2018-2019 (29 mei 2019) vergadernr. 87, item 5, p. 2-3; HTK 2018-2019 (16 oktober 2018) Kamerstuk 35000-VII, nr. 36, p. 5.
- 3 HTK 2015-2016 (12 januari 2016) vergadernr. 40, item 10, p. 5.
- 4 HTK 2017-2018 (4 oktober 2017) vergadernr. 8, item 8, p. 2.

Hoofdstuk 6

Een beoordelingskader voor de behandeling van digitale vraagstukken

De analyse van het parlementaire debat over digitalisering de afgelopen vijf jaar heeft inzichtelijk gemaakt welke inhoudelijke en institutioneel-strategische keuzes de Tweede Kamer in het verleden heeft gemaakt. Deze inzichten kunnen de Kamer ook in de toekomst behulpzaam zijn bij het kiezen van een inhoudelijke invalshoek en om haar positie te bepalen.

Het onderstaande beoordelingskader is een inductieve vertaling van deze inzichten. Het dient als voorzet voor een hulpmiddel om het parlementair debat over digitalisering te structureren en de gewenste focus te geven. Door vroegtijdig en scherp te doordenken wat precies de politiek-maatschappelijke dimensie van het voorliggende digitaliseringsproces is, en welke publieke waarden en belangen daarbij in het geding zijn, kan de Kamer haar rol en positie in het debat beter bepalen. Elk nieuw opkomend vraagstuk van digitalisering kan met behulp van een dergelijk beoordelingskader worden gedefinieerd. De publieke waarden en de risico's én kansen die daarmee verband houden, staan in dit beoordelingskader centraal, om het eigen handelen in alle stadia van beleids- en besluitvorming aan te toetsen. Dat kan helpen om te bepalen waar de eigen informatiebehoefte ligt, om hoofd- van bijzaken te scheiden, en om technologische aspecten en uitvoeringskwesties te vertalen naar een vraagstuk van breder politiek- en maatschappelijk belang. Grip op digitalisering, zo is de achterliggende gedachte, ligt voor de Tweede Kamer niet zozeer in meer kennis en expertise, maar in scherpe afbakening en focus op de eigen rol. Dit beoordelingskader is bedoeld als eerste aanzet, met alle ruimte aan de Kamer om de te doorlopen stappen en aandachtspunten zelf verder in te vullen.



Stap 1 – Het vraagstuk definiëren: de politiek-maatschappelijke dimensie bepalen

- Discussies over digitalisering vinden hun oorsprong vaak in concrete aanleidingen:
 - *Technologische innovatie*: er dienen zich nieuwe digitale technieken en toepassingen van digitale technieken en middelen aan;
 - *Casuïstiek*: er worden individuele voorbeelden of incidentele voorvallen gesignaleerd waarin digitalisering kansen en/of risico's biedt;
 - *Uitvoeringskwesaties*: er blijken zich op het uitvoeringsniveau mogelijkheden en/of problemen voor te doen waarin digitalisering een bepalende rol speelt;

Aan welke bredere politiek-maatschappelijke vraagstukken raken deze innovaties, voorbeelden of uitvoeringskwesaties?

- Welke publieke waarden, nauw verwant aan grond- en mensenrechten, zijn in het geding?
 - privacy
 - autonomie
 - veiligheid
 - controle over technologie
 - menselijke waardigheid
 - rechtvaardigheid
 - machtsverhoudingen

Of raakt het voorliggende vraagstuk nog aan andere publieke waarden? Zo ja, welke?

Stap 2 – Informeren: beschikbare informatie inventariseren, selecteren en waar nodig aanvullen

- Is er voldoende overzicht over de beschikbare beleidsvoorbereidende informatie, van kabinetswege, hoge colleges van staat, adviesraden, toezichthouders, maatschappelijke organisaties enzovoorts?
- Is er voldoende overzicht over de relevante kennis beschikbaar bij expertisecentra en wetenschappelijke instituten? Biedt deze kennis ook het gewenste inzicht in de ethische en maatschappelijke dimensie van het vraagstuk en de publieke waarden die in het geding zijn, of is daarvoor nadere informatie of studie nodig?
- Is er, al dan niet via een systematische stakeholderanalyse, voldoende zicht op de verschillende belanghebbenden en hun al dan niet tegenstrijdige claims?
- Is inspraak nodig? Zo ja, van welke stakeholders?
- Digitalisering is ook bij uitstek een onderwerp van *multilevel governance*. Is goed in beeld welke bestuursniveaus bij dit vraagstuk betrokken zijn en hoe deze zich ten aanzien van dit vraagstuk tot elkaar verhouden, supranationaal (EU), nationaal en decentraal? Waarop moet de discussie op het nationale niveau van regering en parlement zich derhalve richten?
- Welke wet- en regelgeving en/of Europese richtlijnen en verordeningen zijn van toepassing?

Stap 3 – Relateren: het vraagstuk in breder verband bezien

- Hoe hebben regering en parlement in het verleden over het voorliggende vraagstuk, of vergelijkbare vraagstukken, gesproken en geoordeeld? Welke patronen en lessen worden daaruit zichtbaar?
- Zijn verwante digitaliseringsprocessen aan te wijzen die op dit moment in andere beleidsdomeinen spelen? Zo ja, hoe verloopt de beoordeling daar?
- Welke ministeries en Kamercommissies zijn bij dit vraagstuk betrokken, of zouden betrokken moeten worden?
- Richt de digitalisering in discussie zich primair op 1) het verzamelen van data (mensen meten) 2) het analyseren van data (mensen profileren) of 3) het toepassen van digitalisering (ingrijpen in menselijk gedrag)? Wat verandert er aan de definitie van het vraagstuk wanneer het doel of de toepassing van de voorliggende digitalisering verschuift, of wanneer een koppeling plaatsvindt met andere vormen van digitalisering? Welke toekomstscenario's zijn er denkbaar?

Stap 4 – Taxeren van kansen en risico's

- Digitalisering heeft altijd voor- en nadelen. Elke inzet van digitale technologie biedt concrete kansen en risico's.

	KANSEN	RISICO'S
VOOR DE MARKT (ECONOMISCH)	Procesoptimalisatie en kostenefficiëntie, betere concurrentiepositie, investeringen, werkgelegenheid, onderzoek en innovatie, startups, nationale welvaart, ...	Verlies van arbeidsplaatsen, concurrentiedruk door globalisering, marktverstoring door strenge regulering, copyrights, ...
VOOR DE OVERHEID (BESTUUR EN BELEID)	Procesoptimalisatie en kostenefficiëntie, proactieve overheidsinterventies en beter beleid dankzij prognoses en risicoanalyses aan de hand van big data (klimaat, veiligheid e.d.), verbetering van dienstverlening, maatschappelijk draagvlak voor het publieke stelsel, kwaliteitsimpuls in vitale maatschappelijke sectoren, schaalvergroting, ...	Oncontroleerbare data, expertpolitiek, onttrekking aan nationale overheid, ondergraving democratische beleids- en besluitvorming, publiek wantrouwen, ...
VOOR SAMENLEVING EN BURGER (DEMOCRATIE EN AUTONOMIE)	Inspraak, participatie en burgerbetrokkenheid, transparantie, informatievoorziening, persoonlijke autonomie en regie, individueel maatwerk, groei digitale en sociale communicatie...	Ongelijkheid, in- en uitsluiting, anonimisering, verlies van autonomie en keuzevrijheid, privacybeperking, oncontroleerbaarheid, digitale dreiging, desinformatie, ...

- Zijn de kansen en risico's van het voorliggende vraagstuk beide goed in beeld, en worden ze in onderlinge samenhang in het debat betrokken?

Stap 5 – Positioneren: reactie formuleren, positie kiezen en oordeel vormen

- Hoe laat de taxatie van kansen en risico's zich in het voorliggende geval het beste vertalen in concrete beleids- en besluitvorming?
- Hoe zal deze beleids- en besluitvorming uiteindelijk beantwoorden aan de publieke waarden die in het geding zijn?
- Wat is hierin de positie en rol van de Tweede Kamer? Welke handelingsopties liggen voor?
 - Informierend/controlerend;
Is er eerst nadere informatie gewenst, en zo ja, op welk vlak?
 - Agenderend;
Welke aspecten moeten worden aangekaart?
 - Medebeleidsbepalend;
Wat moet er worden bijgestuurd of nader ingevuld?
 - Regulerend/medewetgeving;
Moet er (ook) wet- en regelgeving worden aangepast, en zo ja, welke?
 - ...
- Welke rol is hier naar het oordeel van de Tweede Kamer weggelegd voor de regering?
- Welke rol is er mogelijk weggelegd voor andere bestuursniveaus, uitvoeringsinstanties en/of toezichthouders?
- Op welke manier wil de Tweede Kamer de uitvoering van het genomen besluit en de verdere beleidsvorming blijven volgen?

Bijlage 1

Open data

BESCHRIJVING	Open data zijn digitale gegevens die vrij toegankelijk zijn en zonder beperkingen kunnen worden hergebruikt. Het gaat niet alleen om overheidsinformatie die digitaal beschikbaar is, maar juist ook om de onderliggende ‘ruwe’ data. Open data maken de overheid voor burgers transparanter en toegankelijker én stellen ondernemers in staat om nieuwe toepassingen te ontwikkelen. Tegelijkertijd roept het vragen op met betrekking tot de privacy van persoonsgegevens. Het onderwerp komt in 2011 op de agenda van de Tweede Kamer en krijgt met name tussen 2014 en 2016 veel aandacht.
PUBLIEKE WAARDEN	Transparantie, privacy, kansengelijkheid
MAATSCHAPPELIJKE VRAAGSTUKKEN	Toegankelijkheid van overheidsinformatie, gegevensbescherming
MINISTERIES	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

1. Het verloop van het debat

In 2012 wordt de initiatiefwet Wet open overheid (Woo) ingediend door Tweede Kamerlid Peters (GL) en na haar vertrek uit de Tweede Kamer voortgezet door Voortman (GL) en Schouw (D66). Het doel van deze wet is om overheden en semioverheden transparanter te maken door ervoor te zorgen dat overheidsinformatie vindbaar, uitwisselbaar en eenvoudig te ontsluiten en archiveren is. De Woo moet de Wet openbaar bestuur (Wob) gaan vervangen.

Naar aanleiding van een Europese richtlijn uit 2013, wordt in 2015 het wetsvoorstel Wet hergebruik overheidsinformatie (Who) aan de Kameragenda toegevoegd. In juni 2015 vindt een plenair debat plaats over de Who, waarin onder meer de verhouding tot de Woo wordt besproken. De Who treedt in juli 2015 in werking. Het wetsvoorstel Woo wordt in april 2016 door de Tweede Kamer behandeld en aangenomen. De Eerste Kamer schort de behandeling vervolgens op, om ruimte te geven aan onderzoek naar de impact van de Woo voor overheden.

In november 2015 wordt in een AO van de Tweede Kamercommissie van Binnenlandse Zaken de Nationale Open Data Agenda (NODA) besproken met minister Plasterk. Het debat gaat

met name over de volgens de Tweede Kamer trage ontsluiting van open data door de ministeries. De opvolger van de NODA, het Actieplan Open Overheid (september 2016), zet in op het actief beschikbaar stellen van overheidsdata en het stimuleren van een open houding en gedrag bij overheden. In het VAO wordt onder meer een motie ingediend over de verplichting van open standaarden. Digitalisering van de overheid wordt tijdens een wetgevingsoverleg van Binnenlandse Zaken in oktober 2018 als een centraal thema in de begroting behandeld.

In januari 2019 ontvangt de Eerste Kamer een novelle tot wijziging van dit initiatiefvoorstel, opgesteld door Snels (GL) en Van Weyenburg (D66). Om de zorgen bij overheden weg te nemen, wordt de wet nu verduidelijkt en de uitvoerbaarheid verbeterd. Het wetsvoorstel keert naar verwachting in 2020 terug op de parlementaire agenda. Vanaf 2018 wordt de beschikbaarheid van het Handelsregister van de Kamer van Koophandel (KvK) als open data een punt van discussie in het kader van privacy. De Tweede Kamer organiseert naar aanleiding hiervan in april 2019 een rondetafelgesprek over het databankenrecht. In mei vindt een plenair debat plaats over de toegankelijkheid van het Handelsregister. Langer dan bij andere dossiers, waren regering en Tweede Kamer in deze casus

eensgezind in hun focus op de mogelijkheden van open data voor de overheid zelf, voor semioverheden en bedrijfsleven. Pas de afgelopen paar jaar sloeg de stemming om van efficiëntie en commerciële kansen naar zorgen over privacy en misbruik van gegevens.

2. De informatiepositie van de Tweede Kamer

De Tweede Kamer had door haar eigen initiërende rol bij de Woo een sterke informatiepositie in het debat over open data. Hierdoor kon zij ook druk zetten op de regering om de ontsluiting van overheidsdata daadkrachtig aan te pakken. De talrijke informatiebronnen en de complexe aard van het open data dossier zorgden echter ook voor een gebrek aan overzicht in het Tweede Kamerdebat.

Een belangrijke bron van informatie voor de Tweede Kamer waren de rapporten en adviezen van onder meer het Rathenau Instituut, de Rekenkamer, de Wetenschappelijke Raad voor het Regeringsbeleid en de Raad van State. Het *Tendrapport Open Data* van de Rekenkamer (maart 2014) werd door Voortman (GL) als steun gebruikt voor de initiatiefwet (Woo), omdat hierin

Kamerleden werd de technische kant van deze ontwikkelingen als erg ingewikkeld beschouwd.

De complexe aard van het open data dossier zorgde in juni 2015 voor verwarring in de Tweede kamer over het wetgevingstraject van de Woo en de Who, die in juli 2015 in werking zou treden. Een derde bijkomstigheid was de Wet voorkoming misbruik Wet openbaar bestuur, die in dezelfde maand besproken werd. Het was de Tweede Kamer onduidelijk hoe deze wetten zich precies tot elkaar verhielden en Minister Plasterk werd gevraagd om dit te verduidelijken.

3. De rol van de Tweede Kamer

Sinds 2011 was er een duidelijke ontwikkeling te zien in de rol die Tweede Kamer aannam. Waar ze eerst veel nadruk had gelegd op haar medewetgevende taak (de initiatiefwet Woo), nam ze daarna een meer controlerende rol op zich, die echter wel gepaard ging met bijsturen door middel van moties.

In het AO in juni 2015 waren er zorgen in de Tweede Kamer bij de SP en de PVV over de ondernemers die rijk zouden worden met openbare gegevens van de overheid, maar niet extra belast werden op de winst die ze daarmee maakten. De PVV en de SP drongen erop aan dat de overheid hier ook financieel van zou moeten profiteren. Dit leidde tot een breder debat over de rol van de overheid in de digitale samenleving. Oosenbrug (PvdA) en minister Plasterk betoogden dat het enkel de taak van de overheid was om pre-competitieve informatie te verschaffen en dat het aan de burger was om hierin te investeren.

In haar controlerende taak stelde de Tweede kamer zich kritisch op ten opzichte van de regering, die de urgentie van de Tweede Kamer in de ontsluiting van data niet altijd deelde. Dit leidde ertoe dat de Tweede Kamer door moties en in debatten de regering aanmaande vaart te zetten achter het plannen en uitwerken van open data ambities. De voornaamste kritiek op de regering bleef gedurende de ontwikkeling van het open data debat de beperkte snelheid waarmee ze haar open data ambities waar zou maken.

‘Ik wilde voorstellen hoe we van die digitale dorheid naar een online-oase gaan.’

TWEDE KAMERLID VERHOEVEN (D66) –
16 OKTOBER 2018

diverse kansen van open data werden gesignaleerd. De grote hoeveelheid beschikbare informatie leidde soms ook tot een vernauwing van het debat tot technische vraagstukken. Het aantal digitaliseringwoordvoerders in de Tweede Kamer was beperkt en zij die een achtergrond hadden in ICT, maakten gebruik van hun kennis in het debat. Zo ondersteunde Tweede Kamerlid Oosenbrug (PvdA) in debatten over open standaarden haar (tegen)argumenten met technische kennis van opensourcesoftware. Door andere Tweede

4. Definitie en aandachtspunten

De Tweede Kamer hanteerde geen precieze definitie van digitalisering in het debat over open data. Er was juist een besef dat digitalisering een complex en alomvattend vraagstuk was, dat zich niet scherp liet inkaderen en dat een rol speelde op talrijke beleidsterreinen. De Tweede Kamer benaderde het open data vraagstuk zowel vanuit een technische als een waardengerichte invalshoek.

De technologische invalshoek maakte digitalisering behapbaar voor Tweede Kamerleden met een achtergrond in ICT, maar vormde een drempel voor de meerderheid van de Tweede Kamer. Staatssecretaris Knops van Binnenlandse Zaken en Koninkrijksrelaties merkte in 2018 echter op dat technologische kennis niet noodzakelijk is en dat begrip van de maatschappelijke impact van de techniek belangrijker is.

De waardengerichte invalshoek was vanaf het begin zichtbaar in het Tweede Kamerdebat: transparantie van overheidsdata werd verbonden aan de democratische rechten van de burger. Om deze transparantie te bereiken werd niet uitsluitend over de wettelijke kant ervan gesproken, maar ook in bredere zin over de noodzaak van een verandering in de houding van (semi-) overheden. Deze verandering reikte verder dan het open data dossier. Er moest volgens de Tweede Kamer een verandering van perspectief plaatsvinden, om de digitalisering van de samenleving en de overheid, die als onvermijdelijk werd beschouwd, in goede banen te leiden.

5. Waarden, kansen en risico's in het debat

De Tweede Kamer sprak over open data met name in termen van kansen. De twee voornaamste mogelijkheden werden gezien in de democratische functie die open data zou kunnen vervullen en in de economische meerwaarde voor ondernemers. Op dit laatste terrein kwam in 2018 ook oog voor risico's en de bedreiging van publieke waarden.

Wat betreft de afweging van kansen en bedreigingen die de Tweede Kamer maakte, was het opvallend dat er brede consensus bestond over de mogelijkheden die open data kunnen bieden voor de democratische rechtsstaat,

‘Maar wat duidelijk is, is dat ICT of digitalisering niet meer iets is van “erbij”. Het is gewoon core business van de overheid.’

STAATSSECRETARIS KNOPS – 18 OKTOBER 2019

namelijk transparantie en, in het verlengde hiervan, controle op en eventueel inspraak in overheidsbeleid. Over de economische meerwaarde van open data bestond in 2015 enkel nog onenigheid over de vraag of de overheid hiervan mag meeprofiteren.

Pas later kwam er in de Tweede Kamer ook oog voor eventuele risico's van open data, in het bijzonder met betrekking tot de vermarkting ervan. Het Handelsregister van de Kamer van Koophandel werd een discussiepunt in dit kader. De verstrekking van gegevens uit het Handelsregister vormde het verdienmodel van de Kamer van Koophandel en de instelling wilde daarom zeggenschap houden over deze gegevens. De Tweede Kamer streefde echter naar een open handelsregister en realiseerde dit in de zomer van 2016 door middel van een app. Vanwege privacywetgeving werden sommige gegevens niet opgenomen, maar in 2018 constateerde minister Hoekstra van Financiën dat deze gegevens op werden gekocht door bedrijven, om vervolgens weer te worden doorverkocht. Privacy begon een rol te spelen in het debat. In juni 2019 werd het wetsvoorstel wijziging Handelsregister aangenomen in de Tweede Kamer met als doel het recht op privacy beter te waarborgen.

Ook de waarden kansengelijkheid en veiligheid kwamen aan bod in het Tweede Kamerdebat.

Het achterblijven van een grote groep mensen die niet mee konden komen in de digitalisering van de overheid, werd door verschillende partijen benoemd. Waar andere partijen deze tweedeling wilden voorkomen door te pleiten voor de handhaving van een analoge contactmogelijkheid met de overheid voor de burger, moedigde Tweede Kamerlid Verhoeven (D66) het kabinet aan geen dubbele wegen aan te leggen tussen burger en overheid.

Tweede Kamerlid Amhaouch (CDA) plaatste in september 2016 ook een kanttekening bij het ontsluiten van zo veel mogelijk data en verbond deze aan de publieke waarde veiligheid. Hij verwees daarbij naar het specifieke voorbeeld van mensen met 'slechte bedoelingen', die bijvoorbeeld aan plattegronden van kerncentrales zouden kunnen komen.

Belangrijkste bronnen

Parlementaire documenten

- HTK 2014-2015 (3 juni 2015) vergadernr. 91, item 6.
 HTK 2015-2016 (8 december 2015) Kamerstuk 32802, nr. 22.
 HTK 2016-2017 (7 september 2016) Kamerstuk 32802, nr. 30.
 HTK 2016-2017 (4 oktober 2016) vergadernr. 7, item 24.
 HTK 2018-2019 (16 oktober 2018) Kamerstuk 35000VII, nr. 36.
 HTK 2018-2019 (18 oktober 2018) vergadernr. 15, item 16, p. 7.
 HTK 2018-2019 (31 oktober 2018) Kamerstuk 26643, nr. 579.
 HTK 2018-2019 (29 mei 2019) vergadernr. 87, item 5.

Rapporten en overige documenten

- Open data, open gevolgen*. Nederlandse School voor Openbaar Bestuur (Den Haag 2012).
Tendrapport Open data. Algemene Rekenkamer, 25 maart 2014 (jaarlijks: 2015, 2016).
Steen voor steen de rivier over. Andersson Elffers Felix, 13 oktober 2015.
Ongevraagd advies over de effecten van de digitalisering voor de rechtsstatelijke verhoudingen. Raad van State, 31 augustus 2018.



Bijlage 2

Cybersecurity

BESCHRIJVING	De digitale analyse laat zien dat de hack bij DigiNotar in 2011 een belangrijk referentiekader vormt voor de Tweede Kamer in het debat over cybersecurity. Dat debat wordt met name tussen 2017 en 2019 gevoerd. Voor ons onderzoek is cybersecurity vooral relevant omdat het raakt aan publieke waarden als (nationale) veiligheid, privacy en controle over technologie. Bovendien kunnen we aan de hand van dit debat het krachtenveld rond digitaliseringsvraagstukken onderzoeken. Naast verschillende ministeries (Buitenlandse Zaken, Justitie en Veiligheid, Binnenlandse Zaken en Koninkrijksrelaties, Onderwijs, Cultuur en Wetenschap, betreft dit onder meer de internationale 'techreuzen', een organisatie als het National Cyber Security Centrum en samenwerking in EU-verband.
PUBLIEKE WAARDEN	Privacy, veiligheid, controle over techniek
MAATSCHAPPELIJKE VRAAGSTUKKEN	Veiligheid digitale communicatie tussen burger en overheid; desinformatie verkiezingen; burgerprivacy versus nationale veiligheid
MINISTERIES	Justitie en Veiligheid/Veiligheid en Justitie, Binnenlandse Zaken en Koninkrijksrelaties, Buitenlandse Zaken, Onderwijs, Cultuur en Wetenschap

1. Het verloop van het debat

Cybersecurity is een containerbegrip, en dat maakt het debat erover zeer diffuus. Omdat het onderwerp aan zo veel verschillende beleidsterreinen raakt, wordt het in meerdere Tweede Kamercommissies besproken. Het Tweede Kamerdebat rondom cybersecurity heeft bovendien betrekking op een breed scala aan risico's en bedreigingen. Tot 2017 richt het debat zich voornamelijk op het digitale contact tussen overheid en burgers, waarna een verschuiving optreedt naar internationale vraagstukken en gevaren voor de democratie, en naar bedreigingen van de vitale infrastructuur.

Uit de mediaberichtgeving over cybersecurity blijkt dat in september 2011 de publieke en politieke discussie erover losbarst. Een hack bij Diginotar, een privaat bedrijf dat digitale beveiligingscertificaten uitgeeft aan overheidsdiensten, zorgt ervoor dat honderden overheidswebsites niet langer betrouwbaar zijn. De Tweede Kamer plaatst het dossier op de agenda en een voorstel tot een parlementair onderzoek wordt eind november 2011 door alle fracties ondersteund. Dit onderzoeksvoorstel wordt uiteindelijk overgedragen en geïntegreerd in het

parlementair onderzoek naar ICT-projecten bij de overheid, uitgevoerd door de Commissie Elias. Sinds de Diginotar-crisis blijft cybersecurity op de Tweede Kameragenda staan.

In de jaren na de Diginotar-crisis ligt het accent van kabinet en Tweede Kamer op het veiliger maken van het digitale contact tussen overheid en burgers. In januari 2012 wordt het Nationaal Cyber Security Centrum (NCSC) geopend en in april van dat jaar debatteert de Tweede Kamer over de veiligheid van overheidswebsites. Dat debat leidt onder meer tot het uitvoeren van ICT-beveiligingsassessments van DigiD. Minister Opstelten (Veiligheid en Justitie) komt in de jaren daarna met jaarlijks terugkerende publicaties over cybersecurity, zoals de Nationale Cyber Security Strategie en het Cyber Security Beeld Nederland. Deze publicaties worden tijdens de begrotingsbehandeling van het ministerie in de Tweede Kamer besproken.

Vanaf 2017 krijgt cybersecurity een meer internationale én een democratische dimensie. De Tweede Kamer debatteert in februari over de Wet inlichtingen- en veiligheidsdiensten (Wiv), waarin de gewenste rol van de inlichtingendiensten bij het beschermen van burgers tegen buitenlandse cyberaanvallen centraal staat. In aanloop

naar de Tweede Kamerverkiezingen van maart spreken de parlementariërs naar aanleiding van een onderzoek door RTL Nieuws over de veiligheidsrisico's voor het democratisch proces van elektronisch stemmen. In 2018 volgt het debat over en de implementatie van de Europese Richtlijn voor netwerk- en informatiebeveiliging (NIB) in de Wet beveiliging netwerk- en informatiesystemen. Het jaar 2019 staat vanuit cybersecurity-perspectief vooral in het teken van debatten over (buitenlandse) desinformatie en de bescherming daartegen, met name rondom de Provinciale Statenverkiezingen van maart. De internationale en democratische dimensies komen hier opnieuw bij elkaar.

2. De informatiepositie van de Tweede Kamer

Ten aanzien van cybersecurity heeft de Tweede Kamer met name gebruikgemaakt van drie informatiebronnen. Ten eerste schriftelijke kabinetsinformatie. Regeringsbrieven zijn de voornaamste informatiebron van de Tweede Kamer tijdens de AO's over cybersecurity, maar ook uit rapporten als het *Cyber Security Beeld Nederland* wordt intensief geput.

Ten tweede hebben de Tweede Kamerleden in hun informatiebehoefte voorzien door rapporten te raadplegen van kennisinstituten en adviesraden. Tijdens de debatten over de veiligheid van elektronisch stemmen wordt bijvoorbeeld gerefereerd aan een rapport van de Kiesraad uit 2013 (Commissie Van Beek, *Elke stem telt*), en het debat over vitale waterwerken wordt gevoerd aan de hand van het rapport *Digitale dijkverzwaring* van de Algemene Rekenkamer. Bij de debatten over desinformatie spelen publicaties van de Universiteit Utrecht (*Op weg naar een weerbare open samenleving*, 2018) en de Universiteit van Amsterdam (*De verspreiding van desinformatie via internetdiensten en de regulering van politieke advertenties*, 2019) een rol.

Ten derde agenderen de media regelmatig vraagstukken rondom cybersecurity, waarvan Tweede Kamerleden in debatten wederom dankbaar gebruikmaken. Die agenderende rol van

de media kwam het beste naar voren in aanloop naar de Tweede Kamerverkiezingen van 2017, toen RTL Nieuws concludeerde dat de Ondersteunende Software Verkiezingen (OVS) niet veilig was. Voor zowel Minister Plasterk (BZK) als de Tweede Kamer kwam dit als een verrassing.

3. De informerende, agenderende en regulerende rol van de Tweede Kamer

In de debatten over cybersecurity vertolkte de Tweede Kamer in meer of mindere mate informerende, agenderende en regulerende rollen. Zo zetten de parlementariërs direct na het uitbreken van de Diginotar-crisis al in op hun informerende rol, toen zij opriepen tot een parlementair onderzoek en uiteindelijk unaniem instemden met het onderzoek naar digitale veiligheid van de overheid (eind 2011). Dit onderzoek richtte zich op de wijze waarop overheden de digitale veiligheid beheersten, teneinde het vertrouwen van de burger en de informatiepositie van de nationale overheid te versterken.

De agenderende rol kwam ook regelmatig terug, bijvoorbeeld in een AO in januari 2016 over cybersecurity, waarin Tweede Kamerleden hardop nadenken over een bewustwordingscampagne onder burgers om hun digitale veiligheid te waarborgen. In een AO over nationale veiligheid, een thema dat in eerste instantie vooral betrekking had op overheidstaken, agenderen verschillende parlementariërs de rol van de burger om zelf met cybersecurity aan de slag te gaan. In de debatten over desinformatie rondom verkiezingen in 2019 articuleerden de leden maatschappelijke zorgen omtrent de dubieuze rol van techreuzen als Google en Facebook, en toonden zij zich sceptisch over de in Europees verband gemaakte afspraken met dergelijke bedrijven om hun transparantie te vergroten.

Het kleine gezelschap digiwoordvoerders poogde in het cybersecurity-dossier weliswaar een regulerende rol naar zich toe te trekken in de Tweede Kamer, maar hun moties stuitten dikwijls op een ontrading van de desbetreffende minister of staatssecretaris en/of een ruime Tweede Kamermeerderheid. De

regulerende rol in dit vraagstuk leek vooral samen te hangen met de politieke verhoudingen van het moment. Illustratief is dat D66 als oppositiepartij in december 2016 twee moties – respectievelijk over de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) en software met onbekende kwetsbaarheden – verworpen zag worden, die een klein jaar later integraal in het regeerakkoord van het kabinet Rutte III zouden worden opgenomen. De Europese Unie speelde ook een voorname regulerende rol op het gebied van cybersecurity, waartoe Tweede Kamerleden zich moeten verhouden. De Europese Richtlijn voor netwerk- en informatiebeveiliging (NIB) was in dat kader van belang. Deze richtlijn, die onder andere verplicht tot intensivering van Europese samenwerking, werd door de meeste parlementariërs toegejuicht. Het aannemen van de Nederlandse implementatiewet, de Wet beveiliging netwerk- en informatiesystemen, verliep dan ook zonder veel moeilijkheden.

4. Definitie en aandachtspunten

Net als ‘digitalisering’ is ook cybersecurity een containerbegrip. Het onderwerp komt ter tafel tijdens een keur aan debatten over uiteenlopende thema’s en onderwerpen als arbeidsmarktbeleid, de Wiv, de digitale veiligheid van de Tweede Kamerverkiezingen van 2017, bescherming van de vitale waterwerken en desinformatie rondom de Provinciale Statenverkiezingen van 2019. Het feit dat het onderwerp gedurende de looptijd van deze casus in zo veel verschillende Tweede Kamercommissies de revue is gepasseerd, laat zien dat er uiteindelijk geen duidelijke afbakening is gekomen van het concept cybersecurity.

5. Waarden, kansen en risico’s van digitalisering

Met de ontwikkelingen van digitale technologie nemen hackmogelijkheden en bedreigingen navenant toe. De hoge snelheid waarmee deze ontwikkelingen zich voltrekken, maakt dat de beschermingsmogelijkheden voor burgers, de democratische rechtsstaat en vitale infrastructuur structureel achterlopen. Het vertoog rondom

cybersecurity is dan ook negatief, en gericht op drie categorieën van bedreigingen.

De eerste categorie is die van overheid en burgers en domineerde het cybersecurity-debat van 2011 tot en met 2016. Hierbij ging het in eerste instantie vooral om bedreiging van gevoelige overheidsinformatie door kwaadwillenden. In het verlengde daarvan lag ook de vrees dat te veel vertrouwen in de markt en private digitale beveiligingsbedrijven ertoe zou leiden dat, indachtig Diginotar, gevoelige informatie sneller op straat komt te liggen. Anderzijds was ook het vertrouwen in overheidstoezicht dikwijls beperkt. Zo pleitten de parlementariërs voor versterking van de rol van het in hun ogen nog weinig effectieve NCSC. Privacyrisico’s namen een steeds prominentere positie in het debat over cybersecurity in. De afweging van privacy met (nationale) veiligheid vormde de rode draad in de beraadslagingen van de Tweede Kamer. Soms resulteerde deze afweging in significant verschillende uitkomsten tussen de partijen, zoals tijdens een discussie tussen D66 en VVD over de relevantie van encryptie. Waar eerstgenoemde partij het belang van totale versleuteling (privacy) benadrukte, stelde laatstgenoemde dat nationale veiligheid ‘onder heel strikte voorwaarden’ ten koste mag gaan van burgerprivacy, waarvoor ‘achterdeurtjes’ in de software noodzakelijk zijn.

De tweede categorie was die van de democratische rechtsstaat, die ongeveer eind 2016 opdoemde. Democratische instituties bleken kwetsbaar voor digitale aanvallen, zoals de hacks op het Democratic National Committee aan de vooravond van de Amerikaanse verkiezingen lieten zien. Na berichtgeving van RTL Nieuws concludeerde Minister Plasterk (BZK) dat de veiligheidsrisico’s van stemmen met stemcomputers te groot waren, waarna hij terugkeerde naar een handmatig stemproces met het traditionele rode potlood. De Tweede Kamer beschouwde dit als een juiste beslissing, en koppelde de gebrekkige veiligheid van digitaal stemmen aan de bedreiging van de democratische rechtsstaat. Techgiganten speelden in de ogen van veel parlementariërs een voornamelijk negatieve rol in het debat over cybersecurity en de democratie. Toen minister Ollongren (BZK) begin 2019 meldde dat zij in Europees verband een

code of practice had gesloten met onder meer Google, Facebook en Twitter, bedoeld om hun transparantie te vergroten, leidde dat in de Tweede Kamer vooral tot sceptische reacties.

De derde categorie was die van de fysieke veiligheid, in het bijzonder van de vitale infrastructuur. Deze kreeg in 2019 veel aandacht en kwam duidelijk naar voren in een plenair debat over de vitale waterwerken. Verschillende leden pleitten in dit debat voor ‘pentesten’, het bewust laten hacken van de waterwerken om kwetsbaarheden in de digitale bescherming op te sporen en op te lossen.

De kansen die cybersecurity zou kunnen bieden, werden daarentegen slechts beperkt uitgelicht door de Tweede Kamer. De parlementariërs spraken wél eensgezind over de mogelijkheden die de groeiende cybersecurity-sector kon bieden voor onderwijs en werkgelegenheid.

Belangrijkste bronnen

Parlementaire documenten

- HTK 2015-2016 (20 januari 2016), Kamerstuk 29544, nr. 702.
 HTK 2015-2016 (9 februari 2016), Kamerstuk 33997, nr. 67.
 HTK 2016-2017 (13 december 2016), vergadernr. 34, item 5, p. 1.
 HTK 2016-2017 (8 februari 2017), vergadernr. 50, item 10, p. 1.
 HTK 2016-2017 (9 februari 2017), Kamerstuk 26643, nr. 449.
 HTK 2018-2019 (21 februari 2019), Kamerstuk 22112, nr. 2786.
 HTK 2018-2019 (29 mei 2019), vergadernr. 87, item 9, p. 1.
 HTK 2018-2019 (20 juni 2019), Kamerstuk 30821, nr. 90.
 HTK 2019-2020 (30 oktober 2019), Kamerstuk 30821, nr. 650.

Rapporten en overige documenten

- Cybersecurity Beeld Nederland*. Nationaal Cyber Security Centrum (Den Haag 2012). (vanaf 2012 jaarlijks)
Elke stem telt: elektronisch stemmen en tellen. Kiesraad (Den Haag 2013).
Digitale dijkverzwaring: cybersecurity en vitale waterwerken. Algemene Rekenkamer (Den Haag 2019).
Op weg naar een Weerbare Open Samenleving. USBO (Utrecht 2018).
De verspreiding van desinformatie via internetdiensten en de regulering van politieke advertenties. Instituut voor Informatierecht (Amsterdam 2019).



Bijlage 3

eHealth

BESCHRIJVING	In 2014 worden de doelstellingen van het ministerie voor Volksgezondheid, Welzijn en Sport (VWS) rondom eHealth van kracht. Deze gaan over drie onderwerpen: 1) online inzage in medische gegevens, 2) zelfmeten en gegevensmonitoring en 3) beeldschermzorg en domotica (het automatiseren van processen in huis, denk aan sensoren en camera's). Hierbij kunnen publieke waarden als privacy, veiligheid en menselijke waardigheid in het geding komen en die zijn ook deels in het debat aan de orde gesteld. De breedte van het thema eHealth spreekt uit de verschillende technologische toepassingen die in het debat voorbijkomen, zoals virtual reality (VR) en de ontwikkeling van het Elektronisch Patiëntendossier (epd) en de problemen die hierbij zijn ontstaan. Dit dossier heeft de Tweede Kamer al vroeg bewust gemaakt van het belang om gebruikers en hun behoeften te betrekken bij het ontwerp van een dergelijk systeem.
PUBLIEKE WAARDEN	Privacy, veiligheid, controle over technologie, menselijke waardigheid
MAATSCHAPPELIJKE VRAAGSTUKKEN	Gegevensbescherming, mentale privacy, fysieke patiëntveiligheid, verantwoordelijkheid voor gebruik en opslag gegevens, controle over technologie, instrumentalisering en dehumanisatie van de zorg, toegankelijkheid van de zorg, werkloosheid
MINISTERIES	Volksgezondheid, Welzijn en Sport

1. Het verloop van het debat

In de onderzoeksperiode signaleert de Tweede Kamer dat het tempo van de technologische mogelijkheden in de zorg hoger ligt dan het tempo waarin zorgwet- en regelgeving tot stand komt. Dat tempoverschil leidt er in de eHealth-casus toe dat de kansen van voortschrijdende digitalisering voor het gevoel van de Tweede Kamer onbenut blijven. Het hoge tempo van de technologische ontwikkelingen brengt echter ook de risico's van onvoldoende doordacht digitaliseren aan het licht. De Tweede Kamer uit daarom haar zorgen over de invloed van private partijen en de waarborging van de privacy en veiligheid van de patiënten bij het gebruik van het LSP door zorgverleners.

Het regeerakkoord van Balkenende III (2007) maakt van de toepassing van ICT in de zorg een prioriteit, met name door de invoering van het elektronisch patiëntendossier (epd). In april 2011 strandt het epd in de Eerste Kamer, vanwege zorgen over de waarborging van de privacy. Het regeerakkoord van Rutte II (2012) kondigt aan de kennis en het gebruik van ICT in de zorg te willen vergroten. Hierdoor belandt het thema eHealth in 2012 op de agenda van de Tweede

Kamer als een nieuwe term voor zorginnovatie, al is er wel al eerder over gesproken. In juni 2012 wordt de *Nationale agenda Implementatie eHealth* gepubliceerd. In december 2012 bespreekt de vaste Tweede Kamercommissie voor Volksgezondheid onder andere de doorstart van het epd in het Landelijk Schakelpunt (LSP). Zorgaanbieders kunnen zich aansluiten bij dit 'netwerk' om medische gegevens van patiënten digitaal met elkaar te delen.

De Tweede Kamer focust zich op de winst van betere en meer doeltreffende zorg-op-maat. Eind 2013 dringt zij er bij minister Schippers op aan om invulling te geven aan de ontwikkelingen en mogelijkheden die digitalisering in de zorg biedt. Dit resulteert in de VWS-doelstellingen rondom eHealth in 2014. Deze zijn gericht op 1) online inzage in medische gegevens 2) zelfmeten en gegevensmonitoring en 3) beeldschermzorg en domotica (huisautomatisering en de integratie van technologie en diensten). Tussen 2015 en 2017 spelen vragen omtrent het eigendom van de patiëntgegevens een prominente rol in de commissievergaderingen. Daarnaast houdt deze Tweede Kamercommissie zich bezig met de mogelijkheden van *virtual reality* door de

toepasbaarheid van video games (serious games) in zorgbehandelingen aan te moedigen.

‘Het is van belang dat nieuwe technologie niet alleen wordt gezien als de bekende toys voor boys, maar dat het daadwerkelijk gaat om een andere manier van werken en denken.’

TWEEDE KAMERLID DE LANGE (VVD) –
15 FEBRUARI 2017

Het regeerakkoord van kabinet Rutte III (2017) bevat de belofte te investeren in digitaal ondersteunende zorg om de schaarse capaciteit aan zorgpersoneel optimaal te benutten. De invloed van de media was merkbaar in de discussie, maar die betrof vooral incidenten en de macht van grote techbedrijven. In april 2018 leidt het bericht dat zorgverzekeraars het surfgedrag van hun klanten doorsturen aan Facebook tot Kamerbrede verontwaardiging, wat de impuls versterkt om Kamerbreed over het onderwerp digitalisering in de zorg te spreken. Tijdens een rondetafelgesprek van de tijdelijke commissie Digitale toekomst in september 2019 wordt het epd genoemd als een voorbeeld waarbij het kabinet en de Tweede Kamer bij het maken van beleid onvoldoende aandacht hadden voor de belangen van de gebruikers.

2. De informatiepositie van de Tweede Kamer

De Tweede Kamer beschikte op dit dossier over drie informatiestromen. Ten eerste ontving zij schriftelijke informatie van het kabinet over beleidsplannen en lichtten de bewindspersonen deze mondeling toe tijdens algemene overleggen. Kennisinstituten, adviesraden en belangenorganisaties vormden de tweede

informatiestroom waar Tweede Kamerleden gebruik van maakten. De derde informatiestroom bestond uit initiatieven van de Tweede Kamerleden om in contact te treden met mensen uit het zorgveld. Deze drie informatiestromen gebruikten zij om (de ontwikkeling van) regeringsbeleid te controleren of aan te scherpen. Uit de agenda's van de vergaderingen van de vaste Tweede Kamercommissie voor VWS blijkt dat de Tweede Kamerleden veelvuldig hebben gevraagd om toelichting van de regering in Kamerbrieven over de voortgang van het beleid, interventies van adviesraden of incidenten in de media.

Vanaf 2012 hielp de eHealth monitor van NICTIZ de Tweede Kamerleden om na te gaan of en hoe de technologische ontwikkelingen ingebed waren in de zorgpraktijk en welke behoeften het veld had. De belangrijkste adviesraad was de Raad voor Volksgezondheid. In 2019 bracht de Raad op eigen initiatief en verkennend advies uit over de kansen en risico's van kunstmatige intelligentie in de zorg. Belangenorganisaties zorgden ervoor dat de Tweede Kamer kansen en risico's op dit gebied kon identificeren. Zo bekritiseerde de Patiëntenfederatie de bescherming van persoonsgegevens in de wetgeving en hield de Katholieke Bond van Ouderen een pleidooi voor tablets voor alle ouderen.

De vaste commissie voor VWS organiseerde hoorzittingen/rondetafelgesprekken over het gegevensbeheer van het LSP en het uitgangspunt 'de juiste zorg op de juiste plek', waar een Taskforce onder leiding van VWS aan werkte. In recente debatten putten Tweede Kamerleden daarnaast steeds meer uit werkbezoeken. Tijdens deze bezoeken lieten zij zich informeren over welke lokale initiatieven zorginstellingen opzetten en wat de behoeftes van de zorgaanbieders en gebruikers waren.

3. De rol van de Tweede Kamer

De Tweede Kamer concentreerde zich enerzijds op druk zetten op de regering om vaart te maken met het benutten van de kansen die digitalisering in de zorg bood, terwijl zij parallel daaraan aandacht had voor de risico's

omtrent de digitale uitwisseling van medische persoonsgegevens.

In een motie meende het Tweede Kamerlid Bruins Slot (CDA) dat de regering nog onvoldoende invulling gaf aan de ontwikkelingen en mogelijkheden binnen het zelfmanagement in de zorg, zoals domotica, mobile en eHealth. De Tweede Kamerleden Veldman (VVD) en Dik-Faber (CU) dienden een motie in die stelde dat de potentie van digitale medische technologie groot is en Flevoland een gebied is waar het uitrollen van bestaande, bewezen effectieve ehealth-toepassingen een goede aanvulling kan zijn op het zorglandschap.

Wat betreft reguleren besteedde de Tweede Kamer ook vooral in positieve zin aandacht aan de doeltreffendheid, effectiviteit en de coördinatie van het zorgaanbod. Het amendement van VVD-Tweede Kamerlid De Lange stelde bijvoorbeeld de vraag of de evaluatie van de doeltreffendheid en de effectiviteit van de bekostiging van anonieme e-mentalhealth in de praktijk kon worden teruggebracht naar twee jaar. Ook deed de Tweede Kamer een oproep aan de regering om een centraal digitaal punt in te richten dat een overzicht biedt van goed werkende zorgapps. Veldman (VVD), Van den Berg (CDA) en Bergkamp (D66) dienden moties in over een inventarisatie van bewezen kosteneffectieve digitale innovaties en eHealthtoepassingen en over het opnemen daarvan in de zorgrichtlijnen.

Naast alle optimisme en rol als druk op de regering, heeft de Tweede Kamer ook een waarschuwendende rol op zich genomen. Van den Berg (CDA) waarschuwde in haar initiatiefnota over zorg in de regio voor de trend, waarin de inzet van digitale technieken voor zelfzorg en thuismonitoring in haar ogen samenging met een dreigende verschraling van het zorglandschap.

Het LSP heeft tegenstrijdige moties van Tweede Kamerleden opgeleverd tussen de regeringspartijen en de linkse oppositie partijen. In juni 2018 dienden de coalitiepartijen een motie in, waarin zij de regering verzochten om te onderzoeken of het mogelijk was een wettelijke basis te creëren voor het verplichten van een goede, verantwoorde en veilige elektronische gegevensuitwisseling

tussen zorgaanbieders, zodat de werkdruk omlaag zou gaan. In februari 2019 dienden de Tweede Kamerleden Van Kooten-Arissen (PvdD) en Hijink (SP) daarentegen een motie in, waarin zij constateerden dat het epd qua privacyvereisten in 2011 tekortschoot en het LSP anno 2019 nog steeds tekortschiet. De linkse oppositie was niet perse tegen het LSP, maar wilde dat deelname vrijwillig bleef.

Tijdens discussies over de bescherming van persoonsgegevens probeerden Tweede Kamerleden nadrukkelijk de technologie buiten beschouwing te laten als ze hun punt hierover maakten, omdat zij niet wilden ‘verzanden’ in een discussie over techniek. Hierdoor bleek duidelijk dat het niet zozeer uitmaakte *hoe* het kwam dat persoonsgegevens onvoldoende waren beschermd, maar dat het eenvoudigweg onacceptabel was dat vertrouwelijke medische dossiers in de publieke ruimte waren beland.

4. Definitie

Tweede Kamerleden stuurden erop aan om van eHealth een integrale component te maken in nieuwe zorgwetgeving en het niet als een losstaand project te behandelen. De aandacht van de Tweede Kamer ging uit naar drie thema's:

‘Tegen de tijd dat er één app onderzocht is, zijn er alweer tien bijgekomen en is de eerste alweer verouderd.’

TWEDE KAMERLID AGEMA (PVV) –
7 DECEMBER 2019

kostenbesparende procesinnovatie, zorg-opmaat en gegevensuitwisseling. Zij merkte op dat eHealth de manier was om de kwaliteit van de zorg voor diverse groepen gebruikers en op diverse locaties te borgen voor de langere termijn, op een financieel verantwoorde manier.

Tweede Kamerleden redeneerden sterk vanuit de technische mogelijkheden die benut moesten worden, want daarvan profiteerden uiteindelijk alle betrokkenen – de patiënt, de zorgverlener en de premiebetaler. Daarnaast had de Tweede Kamer oog voor de risico's die digitalisering in de zorg met zich meebracht voor de publieke waarden privacy, veiligheid en menselijke waardigheid.

5. Waarden, kansen en risico's in het debat

Tijdens debatten over kostenbesparende procesinnovatie kregen de belangen van zorgverleners (in termen van werkdruk) een centrale plaats in het debat. Investerings in digitaal ondersteunende zorg hielpen om de zorg betaalbaar te houden. De teneur in de debatten vertoonde overeenkomsten met het debat over SyRI, in die zin dat de effectiviteit van de nieuwe technologie de aandacht had van de Tweede Kamer. Was bijvoorbeeld voldoende bewezen dat de inzet van anonieme e-mentalhealth resultaat opleverde, voordat de Tweede Kamer met de bekostiging instemde? Tegelijkertijd waarschuwden Tweede Kamerleden ervoor dat zorg mensenwerk is en moest blijven: technologische innovatie moest dit mensenwerk ondersteunen en niet vervangen of juist zwaarder belasten.

Aan de andere kant was de Tweede Kamer van mening, dat de implementatie van mogelijkheden van technologische vernieuwingen in de zorgpraktijk snel moest plaatsvinden. De Tweede Kamerleden wilden doorpakken op dit dossier. Een probleem hierbij was dat richtlijnen vaak aan de basis liggen van de ontwikkeling van nieuwe zorg. Het tempo waarin deze richtlijnen tot stand kwamen, was echter trager dan het tempo waarin de zorgtechnologie werd ontwikkeld. In de vaste commissie van VWS klonk daarom het geluid dat digitaal zorgbeleid ook vroeg om innovatie in de methode van wetgeven.

Bij zorg-op-maat debatten stelde de Tweede Kamer het belang van de patiënt centraal bij de bespreking van wetgeving. Het gelijkheidsprincipe stond hierbij voorop. Zorg moest beschikbaar en

bruikbaar zijn voor mensen van alle leeftijden, ongeacht financiële uitgangspositie, woonsituatie of lichamelijke beperkingen. De toegang tot psychische hulp liet zich bijvoorbeeld door Tweede Kamerleden eenvoudig vertalen naar een debat waarin de publieke waarden (fysieke) veiligheid, privacy en autonomie een prominente rol speelden. Als digitale technologie ervoor kon zorgen dat bedreigde personen anoniem toegang konden krijgen tot psychische hulp, dan moest de wet dat mogelijk maken. Het wetsvoorstel daarover was volgens de Tweede Kamer een mooi voorbeeld van het organiseren van zorg vanuit de vraag en de wensen van mensen in plaats van op basis van het denken vanuit een systeem.

Een terugkerend probleem was de spanning tussen het recht op privacy van de patiënt en het belang dat de patiënt heeft bij toegang tot zijn of haar medische gegevens door zorgverleners. Het streven van de Tweede Kamer naar volledig eigenaarschap van de patiënt over zijn of haar eigen medisch dossier, hing naast privacy sterk aan de publieke waarde controle over technologie. Tevergeefs probeerden enkele Tweede Kamerleden minister Schippers ertoe aan te zetten om de Vereniging van Zorgaanbieders voor Zorgcommunicatie het contract met de Amerikaanse bouwer en beheerder (CSC) van het LSP te laten beëindigen. Zij wezen erop dat het onduidelijk was wie in Nederland verantwoordelijkheid droeg voor de gegevensopslag nu deze in handen was van een buitenlandse firma en welke inspectie (Inspectie voor Gezondheidszorg, Autoriteit Persoonsgegevens of de Nederlandse Zorgautoriteit) de controle hierop uitvoerde.

Incidenten die media-aandacht kregen, versterkten de aandacht die de Tweede Kamer besteedde aan de risico's van digitalisering in de zorg. Het incident rond de medische gegevens van een tv-persoonlijkheid leidde tot Kamervragen en hetzelfde gold voor het bericht dat zorgverzekeraars gegevens doorspeelden aan Facebook en dat gegevensopslag in de cloud betekende dat Google meekeek in het medisch dossier. De Tweede Kamer waarschuwde daarom ook voor de druk die private partijen konden leggen op zorgaanbieders en de politiek om

het tempo waarin de zorg digitaliseerde hoog te houden. Innovatie mocht niet overhaast plaatsvinden, maar moest tot stand komen in een dialoog tussen de beleidsmakers, zorginstellingen en gebruikers, onder toezicht van de Nederlandse Zorgautoriteit.

Belangrijkste bronnen

Parlementaire documenten

HTK 2011-2012 (7 juni 2012) Kamerstuk 27529, nr. 108.

HTK 2013-2014 (29 oktober 2013) vergadernr. 16, item 13, p. 1-47.

HTK 2015-2015 (18 juni 2015) Kamerstuk 32620, nr. 162.

HTK 2015-2015 (27 januari 2016) Kamerstuk 27529, nr. 137.

HTK 2016-2017 (15 februari 2017) Kamerstuk 27529 en 33654, nr. 147.

HTK 2017-2018 (30 mei 2018) Kamerstuk 29515, 32012, 32620 en 27529, nr. 433.

HTK 2018-2019 (30 januari 2019) Kamerstuk 27529, nr. 180.

HTK 2019-2020 (7 november 2019) Kamerstuk 27529, nr. 208.

Rapporten en overige documenten

Samen aan zet! eHealth-monitor 2019.

Waarde(n)volle zorgtechnologie. Een verkennend advies over de kansen en risico's van kunstmatige intelligentie in de zorg. Raad voor Volksgezondheid en Samenleving (Den Haag 2019).



Bijlage 4

ICT in het onderwijs

BESCHRIJVING	Naar aanleiding van een onderzoeksrapport van PricewaterhouseCoopers over de vraag hoe scholen en uitgeverijen omgaan met de privacy van leerlingen voert de Tweede Kamer in 2015 een plenair debat met de bewindspersonen van Onderwijs, Cultuur en Wetenschap over privacy in het onderwijs, en de kansen en risico's die verbonden zijn aan digitalisering in het onderwijs. Dit resulteert uiteindelijk in de wijziging van diverse onderwijswetten. Zo komt er onder meer een regeling tot stand om de persoonsgegevens van onderwijsdeelnemers te beschermen en beveiligen. Mede aan de hand van dit debat kan worden onderzocht hoe de Tweede Kamer eerder in het proces een afweging kan maken tussen de verschillende (democratische) waarden, kansen en risico's die met digitalisering zijn gemoeid.
PUBLIEKE WAARDEN	Privacy, kansengelijkheid
MAATSCHAPPELIJKE VRAAGSTUKKEN	Gegevensbescherming van leerlingen (pseudonimisering), kansen(on)gelijkheid in het onderwijs, digitale vaardigheid van leerling en docent
MINISTERIES	Ministerie van Onderwijs, Cultuur en Wetenschap, Ministerie van Economische Zaken

1. Het verloop van het debat

Rapporten en maatschappelijke onrust zijn sturend voor het Tweede Kamerdebat over digitalisering in het onderwijs. In 2014 ligt de focus van de Tweede Kamer voornamelijk op ICT en de kansen die dit kan bieden. Vanaf 2015 verschuift deze focus van kansen naar risico's. Het privacyvraagstuk domineert het debat. In 2017 en 2018 vindt een verbreding van perspectief plaats. Er wordt een meer afgewogen debat gevoerd ten aanzien van waarden, kansen en risico's. Om tot een evenwichtig beeld te komen van digitalisering in het onderwijs heeft zowel het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) als de Tweede Kamer zich in de afgelopen jaren ingezet om de diverse belangenpartijen in het onderwijsveld te betrekken bij de beleidsvoering. Het Doorbraakproject Onderwijs en ICT (2013-2017) vormt een belangrijke stap hierin. Ook de digitaliseringsagenda voor het onderwijs (2018) is tot stand gekomen door samenwerking tussen diverse partijen.

In 2013 start het Ministerie van OCW samen met de belangenvereniging van het primair onderwijs (PO-raad) en van het voortgezet onderwijs (VO-raad) het Doorbraakproject Onderwijs en ICT. Het doel van het project is om scholen vanaf 2017

beter in staat te stellen om om te gaan met ICT en digitale leermiddelen. Hierbij worden talrijke onderwijspartijen en uitgeverijen, distributeurs, gamingbedrijven, soft- en hardware-leveranciers betrokken. In juni 2014 vindt er een AO plaats van de Tweede Kamercommissie OCW met minister Bussemaker en staatssecretaris Dekker. In het debat staan de kansen van ICT voor het onderwijs centraal en wordt voornamelijk gesproken over financiële drempels, zoals het hoge btw-tarief op digitale leermiddelen.

In de winter van 2014-2015 zorgen berichten in de media voor maatschappelijke onrust over de privacy van leerlingen. De berichten betreffen het rapport *Nulmeting Privacy & Beveiliging. Primair en Voortgezet Onderwijs*, dat in het voorjaar van 2014 door PricewaterhouseCoopers (PwC) aangeboden is aan het Ministerie van OCW. Het Tweede Kamerlid Van Meenen (D66) vraagt naar aanleiding hiervan een debat aan met staatssecretaris Dekker. Verschillende Tweede Kamerleden dienen moties in met betrekking tot privacy en de pseudonimisering van leerlinggegevens. In april 2015 komt dit onderwerp ook aan de orde in het convenant Digitale onderwijsmiddelen en privacy, dat plaatsvindt in het kader van het Doorbraakproject. Pseudonimisering wordt ook hier genoemd als doelstelling.

Na dit debat over privacy in 2014-2015 verschijnt digitalisering in het onderwijs nog nadrukkelijker op de Tweede Kameragenda in het vergaderjaar 2017-2018. Op 1 februari 2017 treedt de wet Pseudonimisering leerlinggegevens in werking. Ten gevolge hiervan komt in het najaar een voorstel tot wijzigingen van een aantal onderwijswetten op de Kameragenda. Het Tweede Kamerdebat in oktober 2017 resulteert in het aannemen van de wetwijzigingen. Voor dit debat laten de Tweede Kamerleden zich mede informeren door het rapport *Doordacht digitaal. Onderwijs in het digitale tijdperk* dat in mei 2017 door de Onderwijsraad is aangeboden aan het Ministerie van OCW. Het rapport vormt ook de aanleiding voor een AO van de Tweede Kamercommissie OCW met ministers Van Engelshoven en Slob van OCW in januari 2018. Dit debat beslaat een breed scala aan vraagstukken verbonden met digitalisering in het onderwijs, waarbij de focus ligt op kansen en risico's. In plaats van de technologie zelf staan publieke waarden centraal, waaronder kansengelijkheid.

In maart 2019 wordt de digitaliseringsagenda *Primair en Voortgezet Onderwijs* gelanceerd als onderdeel van de Nederlandse Digitaliseringsstrategie. De initiatiefnemers zijn het Ministerie van OCW, het Ministerie van EZ, de PO-raad, de VO-raad en Kennisnet (dienstverlener op het gebied van onderwijs en ICT). De speerpunten van de agenda zijn onder meer de digitale vaardigheid van leerlingen en leraren, een veilige infrastructuur en het structureel onder de aandacht brengen van de ethiek van digitalisering in het onderwijs.

2. De informatiepositie van de Tweede Kamer

De Tweede Kamer was voor haar informatievoorziening over onderwijs en digitalisering afhankelijk van rapporten en werkbezoeken. Werkbezoeken van Tweede Kamerleden aan onderwijsinstellingen zorgden ervoor dat onderwerpen die niet door het kabinet of door rapporten werden aangekaart, alsnog hun weg naar de Tweede Kamer vonden. Tweede Kamerlid Rog (CDA) stelde in het AO in

juni 2014 naar aanleiding van een werkbezoek Kamervragen over het ontstaan van een ongelijk speelveld in het onderwijs. Doordat sommige scholen examens digitaal afnamen en anderen schriftelijk, bestond volgens Rog het risico van kansenongelijkheid.

Adviezen en rapporten van adviesraden en kennisinstituten hadden eveneens een sturende rol in de Tweede Kamerdebatten. Het onderzoeksrapport van PwC uit 2014 zette het privacy-aspect van digitale leerlinggegevens op de politieke agenda, ook voor de Tweede Kamer. Dit onderzoek constateerde een veiligheidsrisico bij de opslag en het gebruik van digitale leerlinggegevens. Het rapport werd in april 2014 aangeboden aan het Ministerie van OCW, maar werd niet aan de Tweede Kamer gestuurd. In het debat in januari 2015 toonde de Tweede Kamer grote ontevredenheid over haar informatiepositie ten aanzien van het privacyvraagstuk. Ook het rapport *Doordacht digitaal* uit 2017 was sturend voor het Kamerdebat. Dit rapport clusterde een aantal onderwerpen die door de jaren heen in de Tweede Kamer waren besproken, waaronder kansenongelijkheid, en bracht deze zo op een overzichtelijke en evenwichtige wijze terug de Tweede Kamer in.

3. De rol van de Tweede Kamer

De Tweede Kamer zag voor zichzelf twee taken weggelegd op terrein van digitalisering in het onderwijs: het bijeenbrengen van de verschillende partijen die bij het onderwijs betrokken zijn, en het creëren van goede randvoorwaarden.

Het beleidsterrein onderwijs kent een groot netwerk van belangenpartijen en adviesraden, waarvan de PO-raad en de VO-raad de voornaamste zijn. Deze partijen werden door het Ministerie van OCW betrokken bij het Doorbraakproject ICT en Onderwijs. Dit project was uniek omdat naast de belangrijkste adviesraden en het ministerie, ook belangenpartijen als gamingbedrijven en uitgeverijen rond de tafel zaten. Ook in het Tweede Kamerdebat werd het belang om onder meer leraren en leerlingen te betrekken bij de

ontwikkeling van digitale leermiddelen door verschillende Kamerleden benadrukt.

De toenemende focus op privacy in het onderwijs in 2015 leidde ertoe dat in de Tweede Kamer vragen werden gesteld over de verantwoordelijkheid voor het waarborgen van het recht op privacy. Mede door de betrokkenheid van de diverse belangenpartijen, bestond in de Tweede Kamer een zoekende houding over haar eigen rol hierin. In het AO in januari 2018 presenteerde de Tweede Kamer zich overtuigender. Taken ten aanzien van het gebruik en de toepassing van ICT, waarover in 2014 nog werd gediscussieerd, werden in 2018 nadrukkelijk bij het werkveld zelf neergelegd. De Tweede Kamer zag voor zichzelf de taak weggelegd om wettelijke randvoorwaarden te scheppen met oog voor publieke waarden zoals kansengelijkheid en privacy. Hierbij beriep de Tweede Kamer zich op aanbevelingen van het rapport *Doordacht digitaal* van de Onderwijsraad uit 2017. Het rapport benadrukte namelijk de leidende en faciliterende rol van de Tweede Kamer.

4. Definitie en aandachtspunten

Onder de algemene noemer van ICT of digitalisering stonden in 2014 concrete en zeer uiteenlopende technologieën centraal in het Tweede Kamerdebat. Zo werden digitale leermiddelen zoals simulaties (*virtual reality*) besproken, maar ook rekenmachines en de woordentelfunctie van MS Office. Een eerste definitie van digitalisering die door de Tweede Kamer werd gehanteerd verwees naar het gebruik van digitale instrumenten en middelen. In latere jaren werd digitalisering in toenemende mate beschouwd als een proces, een verandering van de samenleving.

In lijn met deze ontwikkeling breidde het palet aan technologieën dat in de Tweede Kamer werd besproken zich verder uit. In het debat in januari 2018 kwamen onder meer *virtual reality*, de cloud, robotica, Ipad's en Prezi aan bod. Technologie was echter niet langer leidend in dit debat: publieke waarden kwamen centraal te staan. Daarbij kreeg het begrip digitalisering nog een derde, bredere invulling: behalve als een autonoom

maatschappelijk proces, begon de Tweede Kamer het begrip ook op te vatten als een leerdoel in dienst van dat proces: scholieren moesten via ICT in het onderwijs in staat worden gesteld om actief vorm te geven aan het proces van digitalisering in de samenleving. Als lichtend voorbeeld werd genoemd het lesgeven in programmeren.

5. Waarden, kansen en risico's in het debat

Tussen 2015 en 2017 verschoof in het debat over digitalisering in het onderwijs de nadruk geleidelijk van kansen naar risico's, met privacy als meest in het oog springende punt. In 2018 was er sprake van een meer afgewogen behandeling van kansen en risico's. Nu kwamen ook waarden aan bod die eerder geen of weinig aandacht hadden gekregen, in het bijzonder kansengelijkheid.

‘Wie houdt er nu precies toezicht op de privacy van onze kinderen?’

TWEDE KAMERLID YPMA (PVDA) –
21 JANUARI 2015

Toen digitalisering in het onderwijs ter sprake kwam in de Tweede Kamercommissie OCW in juni 2014, lag de nadruk van het debat op kansen. ICT en digitale leermiddelen maakten een individuele benadering en adaptief materiaal in het onderwijs mogelijk. Slechts door Tweede Kamerlid Rog (CDA) werd een risico benoemd, namelijk kansengelijkheid. Verder werd door staatssecretaris Dekker kort genoemd dat er bij scholen vragen waren over de privacy van leerlingen, maar het debat richtte zich op de financiële consequenties van ICT in het onderwijs. De Tweede Kamer stelde geen verdere vragen over privacy.

Vanaf 2015 werd het Tweede Kamerdebat over digitalisering in het onderwijs gedomineerd door het privacyvraagstuk. In 2017 spitste dit zich

verder toe op de kwestie van pseudonimisering van leerlinggegevens. Nadat pseudonimisering wettelijk verankerd was, kwam er ook aandacht voor privacy van leerlingen ten opzichte van hun ouders. Door het digitale leerlingvolgsysteem krijgen ouders steeds meer mogelijkheden om hun kind te monitoren, zonder diens toestemming. Dit onderwerp werd in oktober 2017 terloops benoemd, maar kreeg in de media en in het AO in januari 2018 van de Tweede Kamercommissie OCW meer aandacht.

In 2018 veranderde het perspectief van de Tweede Kamer ten aanzien van digitalisering in het onderwijs. Kansen en risico's werden in een breder licht beschouwd dan in de periode 2015-2017. De focus kwam te liggen op waarden, niet op de technologie zelf zoals in 2014 het geval was geweest. Er ontstond een evenwichtiger debat waarin risico's en kansen beide een plek kregen. Het rapport *Doordacht digitaal* van de Onderwijsraad was sturend in deze verschuiving doordat het diverse kansen en risico's onder de aandacht bracht. In het AO in januari 2018 werden risico's besproken die voorheen geen of weinig aandacht hadden gekregen, zoals digitaal pesten. Ook werden er diverse nieuwe kansen besproken, zoals les op afstand en het lesgeven in programmeren. Kansengelijkheid, in 2014 al benoemd door Tweede Kamerlid Rog (CDA), kwam opnieuw aan de orde. Verschillende partijen vroegen aandacht voor de bedreiging die digitalisering vormt voor de kansengelijkheid in het onderwijs, het gevaar van een zogenoemde digitale kloof.

Belangrijkste bronnen

Parlementaire documenten

- HTK 2013-2014 (11 juni 2014), Kamerstuk 32034, nr. 4.
- HTK 2014-2015 (21 januari 2015), vergadernr. 44, item. 9, p.1.
- HTK 2015-2016 (22 december 2015), Kamerstuk 32034, nr. 19.
- HTK 2017-2018 (4 oktober 2017), vergadernr. 8, item. 8, p.1.
- HTK 2017-2018 (31 januari 2018), Kamerstuk 32034, nr. 30.

Rapporten en overige documenten

- Doordacht digitaal. Onderwijs in het digitale tijdperk.* Onderwijsraad (Den Haag 2017).
- Nulmeting Privacy & Beveiliging Primair en Voortgezet Onderwijs.* PricewaterhouseCoopers (Amsterdam 2014).



Bijlage 5

SyRI

BESCHRIJVING	SyRI (Systeem Risico Indicatie) is een overheidssysteem om persoonsgegevens van burgers te koppelen en te analyseren. Het is vooral bedoeld om socialezekerheidsfraude te bestrijden. De ontwikkeling van SyRI hangt samen met verschillende digitaliseringstrends, zoals het gebruik van big data, algoritmes en artificial intelligence. Het debat over het gebruik van dit systeem richt zich op democratische waarden als privacy en rechtvaardigheid.
PUBLIEKE WAARDEN	Privacy, rechtvaardigheid, controle over techniek
MAATSCHAPPELIJKE VRAAGSTUKKEN	Gegevensbescherming, doelverschuiving technologie, surveillance, discriminatie, stigmatisering
MINISTERIES	Sociale Zaken en Werkgelegenheid, Veiligheid en Justitie/Justitie en Veiligheid, Economische Zaken

1. Het verloop van het debat

Op 1 januari 2014 treedt de Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI) in werking. Het Systeem Risico Indicatie (SyRI) maakt onderdeel uit van deze wet. Het uitgangspunt van SyRI is fraude bestrijden of voorkomen door middel van gegevens die de overheid of andere organisaties met een publieke taak al beschikbaar hebben. Op 12 september 2013 wordt de wet als hamerstuk afgedaan, zonder verdere beraadslaging en stemming. In de schriftelijke voorbereiding die daaraan vooraf is gegaan, heeft het oorspronkelijke wetsvoorstel acht wijzigingen ondergaan – mede om tegemoet te komen aan kritiek van Raad van State en de Autoriteit Persoonsgegevens over de ruime opzet van het systeem en over de beoogde gegevensverzameling. In de Tweede Kamer (en ook in de Eerste Kamer) overheerst echter het beeld van een weinig controversieel wetsvoorstel. Pas drie jaar later barst de publieke en politieke verontwaardiging over onwenselijke effecten van de inzet van het systeem los; dan pas blijkt ook hoezeer de gekozen technologie raakt aan publieke waarden als privacy en rechtvaardigheid.

In de periode van de totstandkoming van de wet maken Tweede Kamerleden zich nog vooral zorgen over de balans tussen de financiële kosten en baten van het systeem. Tijdens een AO in

december 2014 over belastingontduiking en misbruik en oneigenlijk gebruik op het gebied van sociale zekerheid en subsidies, uiten de parlementariërs hun zorgen over de vraag of de kosten van SyRI niet hoger dreigen uit te vallen dan de boete-opbrengst. In een AO in juli 2015 over hetzelfde thema komt SyRI slechts zijdelings ter sprake, en dan alleen in de context van de effectiviteit van het systeem in het opsporen van fraude.

Het WRR-rapport *Big Data in een vrije en veilige samenleving* uit april 2016 markeert het omslagpunt in de toon van het parlementaire debat. De WRR voert SyRI hierin op als een van de zeven casussen waarin data-analyses een hoge vlucht hebben genomen. Naar aanleiding van dit rapport ziet het kabinet zich genoodzaakt hierover een standpunt in te nemen. Het stelt dat de inzet van SyRI aan voldoende randvoorwaarden is gebonden die in lijn zijn met het verbod op geautomatiseerde besluitvorming.

De Tweede Kamer ziet dat anders, en hamert vanaf dat moment steeds meer op bedreigingen voor de privacy, mogelijke discriminatie en het wantrouwen van de overheid tegenover de burger dat uit het systeem lijkt te spreken. Protestacties van maatschappelijke organisaties en alarmerende berichtgeving in de media hebben de Tweede Kamer doen inzien hoe diep het systeem ingrijpt in de persoonlijke levenssfeer. Dit wordt

vervolgens ook het centrale argument in het debat, zoals in een AO in mei 2018. In oktober 2019 roepen verschillende Tweede Kamerleden het kabinet op te stoppen met SyRI. Op 5 februari 2020 vindt die oproep ook juridisch gehoor: de Rechtbank Den Haag concludeert dat SyRI in strijd is met het Europees Verdrag voor de Rechten van de Mens en gebiedt de overheid te stoppen met het systeem.

2. De informatiepositie van de Tweede Kamer

De Tweede Kamer heeft bij het SyRI-vraagstuk met name gebruikgemaakt van drie informatiebronnen: beleidsvoorbereidende documentatie van het kabinet, rapporten van kennisinstituten en adviesraden, en mediaberichtgeving. Gedurende de voorbereiding van het wetsvoorstel zijn de door het kabinet gepresenteerde visie en aangeleverde informatie leidend. Externe rapportages en mediaberichtgeving gaan in het parlementaire debat pas een serieuze rol spelen als de risico's van de nieuwe technologie in beeld beginnen te komen.

De eerste informatiebron waren schriftelijke en mondelinge toelichtingen van het kabinet op het systeem, vooral in de vorm van de memorie van toelichting bij het wetsvoorstel, aangevuld met brieven en reacties in AO's en VAO's. Het belang van fraudebestrijding staat hierin centraal.

Vanaf 2014 beginnen Tweede Kamerleden als tweede informatiebron ook rapporten van kennisinstituten en adviesraden meer in het debat te betrekken. Een eerste voorbeeld hiervan is het rapport *Kennis delen geeft kracht. Naar een betere én zorgvuldige gegevensuitwisseling in samenwerkingsverbanden* (Werkgroep Verkenning kaderwet gegevensuitwisseling, 2014). Van invloed is vervolgens het hierboven al genoemde WRR-rapport *Big Data in een vrije en veilige samenleving* (april 2016). Aan de hand hiervan dwingt de Tweede Kamer het kabinet haar nader te informeren over de data-analyses die door SyRI worden uitgevoerd. De rapporten die daarna in het parlementaire debat worden

aangehaald, sturen de Tweede Kamer nog sterker in de richting van de risico's van het systeem vanuit het perspectief van disproportionele menselijke profilering, aantasting van grondrechten en publieke waarden. De Tweede Kamer put hiervoor met name uit de rapporten *Opwaarderen* (2017) en *Doelgericht digitaliseren* (2018) van het Rathenau Instituut, en daarnaast uit het rapport van de Universiteit Utrecht over *Algoritmes en grondrechten* (2018).

Met de toenemende publieke verontwaardiging over SyRI groeit ook het belang van mediaberichtgeving als informatiebron. De eerste tekenen hiervan zijn eveneens in 2014 terug te vinden, als *de Volkskrant* en Nu.nl berichten over het profileren van burgers door koppeling van data. Deze berichtgeving is voor de vaste Kamercommissie voor Sociale Zaken op 14 oktober 2014 aanleiding om er in een procedurevergadering over te spreken.

‘Je ziet dat het [SyRI] wel degelijk een heel goede bijdrage levert aan het bestrijden van fraude en de aanpak van malafide uitzendbureaus.’

MINISTER ASSCHER – 1 JULI 2015

3. De informerende, agenderende en regulerende rol van de Tweede Kamer

In het SyRI-vraagstuk krijgt de informerende rol van de Tweede Kamer vooral gestalte door regelmatig AO's te beleggen met bewindspersonen en Kamerbrieven te raadplegen. Ook voert de Tweede Kamer op 4 oktober 2017 een dertigledendebat over de digitalisering van infrastructuur met minister Kamp van Economische Zaken. Het debat resulteert in een lijst met vragen naar het gebruik van algoritmen binnen de overheid. Het antwoord op deze vragen krijgt de Tweede Kamer driekwart jaar later

van onderzoekers van de Universiteit Utrecht in het rapport *Algoritmes en grondrechten*. In het algemeen geldt dat de snelheid waarmee digitalisering het functioneren van de overheid beïnvloedt, het voor de Tweede Kamerleden dikwijls lastig maakt om hun informerende rol, en in het verlengde daarvan hun klassieke controlerende taak, goed in te vullen. Tegelijkertijd hebben de Tweede Kamerleden hun kennisachterstand dankzij het inwinnen van expertise relatief snel ingelopen, waarbij vooral de reeds genoemde recente Rathenau-rapporten zeer behulpzaam zijn gebleken.

De agenderende rol van de Tweede Kamer ten aanzien van SyRI komt vanaf 2016 meer tot haar recht. In de jaren daarvoor houden de leden zich nog erg op de vlakte over het systeem, zoals blijkt uit AO's in december 2014 en juli 2015 over misbruik en oneigenlijk gebruik van belastingen, sociale zekerheid en subsidies. De publicatie van het WRR-rapport *Big Data in een vrije en veilige samenleving* (2016) vormt als gezegd het kantelpunt. Vanaf dat moment beginnen Tweede Kamerleden maatschappelijke zorgen rondom privacy en discriminatie volop aan SyRI te verbinden. Als vakbond FNV in de ochtend van 9 oktober 2019 een protest tegen SyRI organiseert op Het Plein in Den Haag, ventileren verschillende Tweede Kamerleden enkele uren later in een AO het wantrouwen van burgers tegenover het systeem.

De regulerende rol van de Tweede Kamer houdt hiermee gelijke tred. Ook wat dit betreft schudt het WRR-rapport uit 2016 de Tweede Kamer wakker. Tijdens een AO over verwerking en bescherming van persoonsgegevens in mei 2018 articuleren meerdere Kamerleden het gevoel dat de Tweede Kamer in het SyRI-dossier onvoldoende inhoud heeft gegeven aan haar medewetgevende rol. Dat heeft de Tweede Kamer sindsdien proberen recht te zetten. Zo hamerde de vaste commissie voor Justitie en Veiligheid in juni 2019 tijdens een AO over de verwerking en bescherming van persoonsgegevens op wettelijke grondslagen voor gegevensdeling, ook indachtig SyRI. Naar het oordeel van minister Dekker liep de Tweede Kamer nu echter te ver voor de troepen uit: dit zou 'pionierswetgeving' betreffen

waarvoor nog veel tijd en juridisch denkwerk nodig was.

4. Definitie

De SyRI-casus onderstreept hoe lastig het soms voor de Tweede Kamer is om een expliciete definitie van digitalisering te hanteren. In de aanloop naar het betreffende wetsvoorstel verbinden de meeste Tweede Kamerleden SyRI helemaal niet aan digitalisering; het gaat dan nog primair om de mogelijkheden die dit systeem biedt om fraude op te sporen en erosie van het draagvlak onder het sociaal zekerheidsstelsel tegen te gaan. Onder invloed van het WRR-rapport over big data, een rondetafelgesprek met de voorzitter van de WRR over kunstmatig intelligentie en het rapport *Opwaarderen* van het Rathenau Instituut – en niet te vergeten de publieke onrust – verandert dit. SyRI wordt dan vooral een vanuit risico's gedefinieerd digitaliseringsvraagstuk: wat zijn precies de maatschappelijke gevaren als de overheid big data met behulp van algoritmes gaat verzamelen en verwerken? Met deze herdefiniëring komt SyRI ook symbool te staan voor een breder politiek en publiek vraagstuk, namelijk hoe ervoor te zorgen dat ook in de digitale samenleving de mensenrechten en daaruit voortvloeiende publieke waarden onverminderd juridisch geborgd zijn.

5. Waarden, kansen en risico's van digitalisering

Het parlementaire debat over SyRI ontwikkelt zich zogezegd langs een klassiek argumentatiepatroon. Het debat vertrekt vanuit kansen en mogelijkheden, maar mondt uiteindelijk uit in een discussie over de risico's. Eerst ligt de nadruk op de functionele en procesmatige voordelen van het systeem, dan pas komen de ethische dilemma's in beeld. In plaats van een instrument dat het *vertrouwen* in de overheid moest versterken – het pakte immers uitkeringsfraude aan – ging de Tweede Kamer SyRI steeds meer zien als iets dat het *wantrouwen* tegenover de overheid aanwakkerde. In lijn hiermee heeft de Tweede Kamer SyRI opgewaarderd tot een

politiek-maatschappelijk digitaliseringsvraagstuk waarbij belangrijke publieke waarden in het geding zijn. In verschillende debatten spreekt de Tweede Kamer haar zorgen uit over discriminatie van mensen op basis van systematische profilering. Onder meer in het AO van mei 2019 gaat het over de vergaande beperking van de persoonlijke levenssfeer die het stempel van potentieel fraudeur met zich meebrengt. Leden schuwen daarbij de grote woorden niet: SyRI dreigt Nederland te veranderen in een surveillancestaat. In deze debatten weerklinkt duidelijk ook de terminologie uit het Rathenau-rapport *Doelgericht digitaliseren*. Vooral de publieke waarden en daaraan verbonden maatschappelijke vraagstukken die hierin worden onderscheiden, helpen de Tweede Kamer om te benoemen waar het SyRI-dossier om draait: het systeem roept niet alleen vragen op over privacy (gegevensbescherming), maar ook over controle over technologie (inzicht in algoritmen) en rechtvaardigheid (anti-discriminatie, omkeerbaarheid besluit, recht op vergissen).

Belangrijkste bronnen

Parlementaire documenten

- HTK 2014-2015 (17 december 2014), Kamerstuk 17050, nr. 501.
- HTK 2017-2018 (4 oktober 2017), vergadernr. 8, item 11, p. 1-11.
- HTK 2017-2018 (30 mei 2018), Kamerstuk 26642 en 32761, nr. 543.
- HTK 2017-2018 (6 juni 2018), vergadernr. 90, item 3, p. 1-5.
- HTK 2018-2019 (13 juni 2019), Kamerstuk 32761, nr. 148.
- HTK 2019-2020 (9 oktober 2019), Kamerstuk 26448, nr. 629.

Rapporten en overige documenten

- Naar een betere én zorgvuldige gegevensuitwisseling in samenwerkingsverbanden*. Werkgroep Verkenning kaderwet gegevensuitwisseling (Den Haag 2014).
- Big Data in een vrije en veilige samenleving*. Wetenschappelijke Raad voor het Regeringsbeleid (Den Haag 2016).
- Opwaarderen*. Rathenau Instituut (Den Haag 2017).
- Algoritmes en grondrechten*. Universiteit Utrecht (Utrecht 2018).
- Doelgericht digitaliseren*. Rathenau Instituut (Den Haag 2018).



Bijlage 6

Overzicht van regeringsagenda's en onderzoeksrapporten

Het onderstaande overzicht bevat de regeringsagenda's en een uitgebreide selectie rapporten van adviesorganen en onderzoeksbureaus gerelateerd aan ICT en digitalisering, verschenen in de periode 1998-2020.

Regeringsagenda's

- *Nederlandse Digitaliseringsstrategie 2.0* (5 juli 2019) – de digitale transitie van Nederland kan alleen slagen door samenwerking. Om die reden heeft het kabinet de Nederlandse Digitaliseringsstrategie gelanceerd. Dit is de eerste keer dat er kabinetsbreed een ambitie en doelstellingen zijn geformuleerd op het terrein van digitalisering.
- *NL Digibeter 2019: Agenda Digitale Overheid* (1 juli 2019) – dit is de eerste geactualiseerde versie van NL Digibeter. De overheid zet de publieke waarden centraal en respecteert de grondrechten. Het rapport formuleert de volgende pijlers: innovatie, data, inclusie, digitale identiteit en regie op gegevens. Bij de uitvoering van de acties groeit het besef dat overheidsorganisaties alleen door samen op te trekken de doelen kunnen realiseren. Dit heeft geleid tot het aanpassen of opstellen van agenda's van medeoverheden.
- *NL Digitaal: Data Agenda Overheid* (28 februari 2019) – de agenda spreekt over de 'dataficering' van de samenleving en beschrijft hoe de mogelijkheden van data ten goede kunnen komen aan beleidsvorming en het oplossen van maatschappelijke vraagstukken door de overheid. Daarnaast wordt nadrukkelijk aandacht besteed aan de bescherming van publieke waarden en fundamentele rechten.
- *Nederland Digitaal: De Nederlandse visie op datadeling tussen bedrijven* (1 februari 2019) – in deze visie ligt de focus niet op de overheid, maar op de bedrijven. Dataverdeling moet meer dan nu gebruikelijk worden. Het kabinet ambieert daarmee dat Nederland vooroploopt met verantwoorde verzilvering van de maatschappelijke en economische kansen van datadeling tussen bedrijven.
- *NL Digibeter: Agenda Digitale Overheid* (13 juli 2018) – de overheid wil de kansen van digitalisering benutten en tegelijkertijd de autonomie van de burger respecteren. De Grondwet en de daaruit voortvloeiende publieke waarden zoals privacy, zelfbeschikking en gelijkheid zijn juist bij de voortschrijdende digitalisering essentieel om te borgen. Het gaat volgens het rapport om een 'rolling agenda' die ieder jaar bijgesteld wordt.
- *Nederlandse Digitaliseringsstrategie: Nederland digitaal* (1 juli 2018) – rapport over wat nodig is om te zorgen dat Nederland sterk blijft op het gebied van digitalisering. Nederland heeft een goede uitgangspositie om economische en maatschappelijke kansen van digitalisering te verzilveren. Tegelijkertijd roept digitalisering ook nieuwe, fundamentele vragen op. Bijvoorbeeld over de bescherming van privacy en werkgelegenheid. Het kabinet zet daarom in op een aanpak van twee sporen: maatschappelijke en economische kansen benutten (versnellen) en versterken van het fundament (basisvoorwaarden).
- *Nederlandse Cybersecurity Agenda: Nederland digitaal veilig* (21 april 2018) – de NSSA valt uiteen in zeven ambities die bijdragen aan de volgende doelstelling: Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en de nationale veiligheid in het digitale domein te beschermen.

- *Digitale agenda: Vernieuwen, vertrouwen, versnellen* (5 juli 2016) – digitalisering wordt meer en meer gezien als de vierde industriële revolutie. Digitalisering is een bron van innovatie, bedrijvigheid en economische groei. Bovendien biedt het nieuwe mogelijkheden voor de aanpak van maatschappelijke uitdagingen. Alleen gezamenlijk kunnen we kansen van de digitale transitie grijpen en de uitdagingen, waar voor we ons gesteld zien, aangaan. De overheid richt zich hierbij niet alleen op het versterken van de randvoorwaarden, maar is zelf ook actor in deze transitie als gebruiker van innovatieve ICT en aanjager van publiek-private samenwerking.
- *Digitale Implementatie Agenda.nl* (16 november 2011) – als vervolg van de Digitale Agenda.nl beschrijft de Digitale Implementatie Agenda.nl voor een aantal acties de verdere implementatie. Voortschrijdende globalisering vraagt om duidelijke strategische profilering van Nederland. Onderzoek laat zien dat Nederland een ‘Digital Gateway to Europe’ is. Voor de uitvoering van de Digitale Agenda.nl is een breed (bestuurlijk) draagvlak nodig en gezamenlijke actie van de overheid en diverse publieke en private partners.
- *Digitale Agenda.nl: ICT voor innovatie en economische groei* (17 mei 2011) – de agenda schetst het ICT-beleid voor de periode 2011-2015. De focus ligt op de bijdrage die ICT kan leveren aan de economische groei in Nederland. Meer ruimte voor ondernemers om slimmer te werken over een snelle en open infrastructuur die met vertrouwen kan worden gebruikt en met kennis die werkt.
- *ICT-agenda 2008-2011: De gebruiker centraal in de digitale dienstenmaatschappij* (6 september 2008) – periodieke herziening van de ICT-agenda uit 2004. Het kabinet heeft als ambitie om Nederland in 2015 te laten behoren tot de koplopers in de beschikbaarheid en het gebruik van ICT-toepassingen en nieuwe digitale dienstverlening. Dit is niet alleen wenselijk vanuit internationale concurrentieoverwegingen, maar ook noodzakelijk om enkele knelpunten in het maatschappelijke domein, waaronder de toenemende zorgvraag en de vraag om meer hoogopgeleide werknemers, het hoofd te bieden.
- *De rijksbrede ICT-agenda: Beter presenteren met ICT* (23 februari 2004) – de eerste rijksbrede ICT-agenda, opgesteld door de ministers van Economische Zaken, Bestuurlijke Vernieuwing en Koninkrijksrelaties en de staatssecretaris van Onderwijs, Cultuur en Wetenschap. Het kabinet wil condities creëren waardoor de samenleving beter in staat is ICT optimaal te benutten. Enerzijds door de betere benutting van ICT door bedrijven, burgers en in (semi-)publieke sectoren, anderzijds door de ICT-basis te versterken. Het gaat dan om de communicatie-infrastructuren, onze ICT-kennispositie en de randvoorwaarden voor een goed, veilig en betrouwbaar gebruik.

Gerelateerde overheidsagenda's

- *Digitale Agenda voor Europa* (19 mei 2010) – in de agenda wordt uiteengezet welke essentiële faciliterende rol ICT zal moeten spelen als Europa zijn ambitieuze doelstellingen voor 2020 wil halen.
- *Digitale agenda (2020)* (juni 2015) – uitwerking van een collectieve gemeentelijke aanpak op het gebied van dienstverlening en informatiebeleid door de VNG (Verenigingen Nederlandse Gemeenten).

Rathenau Instituut

- *Verantwoord virtueel* (19 november 2019) – vier maatregelen om consumenten te beschermen tegen gezondheids- en andere effecten van virtual reality.
- *Burgers en sensoren* (11 september 2019) – dit rapport presenteert acht spelregels voor de inzet van sensoren voor veiligheid en leefbaarheid.
- *Kennis in het vizier* (1 juli 2019) – dit rapport bespreekt de gevolgen van de digitale wapenwedloop voor de publieke kennisinfrastructuur.
- *Griffiers en digitalisering* (14 juni 2019) – dit rapport beschrijft mogelijkheden om de lokale democratie vitaal en sterk te maken.

-
- *Cyberspace zonder conflict* (25 april 2019) – dit rapport onderzoekt mogelijkheden om de escalatie van het internationale informatieconflict te voorkomen.
 - *Gezondheid centraal* (23 januari 2019) – rapport geeft overheid, zorgveld en politiek handvatten om te zorgen dat de inzet van digitale diensten voor gezondheidsdata past bij een maatschappelijk verantwoorde digitale samenleving.
 - *Doelgericht digitalisering* (13 september 2018) – rapport geeft vijf acties om waarden gedreven te vernieuwen.
 - *Beschaafde Bits* (20 juli 2018) – uit het rapport blijkt dat er vier uitgangspunten zijn die de samenleving kunnen helpen beter om te gaan met digitale technologie.
 - *Waardevol digitalisering* (26 juni 2018) – dit rapport geeft tien perspectieven aan lokale bestuurders om maatschappelijk verantwoord te digitaliseren.
 - *Digitale gezondheidsregie* (25 mei 2018) – rapport biedt een inzicht in de kansen en uitdagingen van het streven naar digitale gezondheidsregie.
 - *Digitalisering van het nieuws* (24 mei 2018) – dit rapport laat zien dat vitale functies van de nieuwsvoorziening voor het Nederlandse publieke en politieke debat onder druk kunnen komen te staan.
 - *Robotisering en automatisering op de werkvloer* (2 mei 2018) – rapport laat zien voor welke keuzes bedrijven komen te staan bij de introductie van nieuwe digitale technologie.
 - *Mensenrechten in het robottijdperk* (11 oktober 2017) – in dit rapport pleit het Rathenau Instituut voor een nieuw Europees verdrag met twee nieuwe mensenrechten.
 - *Een nooit gelopen race* (2 maart 2017) – dit rapport laat zien dat de huidige maatregelen van overheid en bedrijfsleven tegen cyberdreigingen niet volstaan.
 - *Regels voor het digitale mensenpark* (23 februari 2017) – de afgelopen jaren is wereldwijd een lappendeken aan regels ontwikkeld om opkomende technologieën in goede banen te leiden. Dit rapport stelt de vraag of de regels ons wel voldoende beschermen.
 - *Opwaarderen* (6 februari 2017) – rapport laat zien dat de overheid, de toezichthouders, het bedrijfsleven en de samenleving niet voldoende zijn toegerust om met de vragen van deze tijd om te gaan.
 - *De controle kwijt* (6 april 2016) – dit onderzoek heeft als doel beleidsmakers te informeren over privacybescherming op het internet.
 - *Digitalisering van dieren* (8 februari 2016) – in dit rapport ligt de focus op het gebruik van smart farming binnen de Nederlandse veehouderij en de mogelijke maatschappelijke vragen die de digitalisering van het boerenbedrijf oproept.
 - *De meetbare mens* (4 februari 2016) – deze bundel gaat over de digitalisering van de gezondheidszorg en de gevolgen voor mens en maatschappij.
 - *Kansen en dilemma's van digitale democratie* (3 november 2015) – uit het rapport blijkt dat er niet alleen kansen zijn voor het Nederlandse e-parlement, maar zeker ook dilemma's.
 - *De datagedreven samenleving* (22 september 2015) – dit rapport brengt de stand van zaken van het debat over de verantwoorde inzet van big data in kaart.
 - *Werken aan de robotsamenleving* (17 juni 2015) – dit rapport gaat over de relatie tussen technologie en werkgelegenheid.
 - *De kracht van platformen* (13 oktober 2014) – dit rapport bespreekt de maatschappelijke en economische betekenis van innoveren in een gedigitaliseerde wereld.
 - *Tem de robotauto* (2 oktober 2014) – deze studie schept duidelijkheid over de verschillende ontwikkelingspaden van de zelfsturende auto.
 - *Veiligheid van systemen voor de digitale overheid* (16 juli 2013) – dit rapport wijst op veelbelovende mogelijkheden voor beleidsontwikkeling in de gedigitaliseerde samenleving.
 - *Voorgeprogrammeerd* (27 maart 2012) – dit rapport beschrijft hoe aanbieders verdienen aan digitale profielen en hoe zij met knoppen, beelden en zinnen je klikgedrag sturen.

- *Van vergeetpil tot robotpak* (5 juli 2011) – deze studie verkent diverse human enhancement technologieën en hun toepassing binnen de gebieden recht en veiligheid.
- *Databases* (17 november 2010) – deze studie laat zien dat het toenemend gebruik van databases in onze gedigitaliseerde samenleving niet zonder risico's is.
- *Check in/check out* (1 juni 2010) – dit rapport bespreekt de digitalisering van de openbare ruimte en de impact daarvan op ons dagelijks leven.
- *Het EPD: opvattingen van burgers* (4 maart 2010) – verslag van een onderzoek naar de opvattingen van burgers over invoering van een landelijk elektronisch patiëntendossier.
- *Medische technologie: ook geschikt voor thuisgebruik* (30 oktober 2009) – in deze studie wordt de ontwikkelingsdynamiek onderzocht die ten grondslag ligt aan de opkomst van de zelfzorgmarkt.
- *Leven als bouw pakket* (1 oktober 2009) – deze bundel verkent de ethische kwesties van een nieuwe technologische golf.
- *De migratiemachine* (1 februari 2009) – deze bundel levert een bijdrage aan het debat over de effectiviteit, de betrouwbaarheid en de proportionaliteit van technologie in het migratiebeleid.
- *Van privacyparadijs tot controlestaat?* (1 februari 2007) – dit rapport geeft een overzicht van de huidige en te verwachten veiligheidsmaatregelen, inclusief het cumulatieve effect daarvan op de privacy van de burger.

WRR

- *Voorbereiden op digitale ontworping* (9 september 2019) – in dit rapport pleit de WRR voor betere voorbereiding op digitale ontworping.
- *Internationaal AI-beleid. Domme data, slimme computers en wijze mensen* (juni 2019) – internationaal AI-beleid wordt onderzocht aan de hand van de gepubliceerde strategieën en aanpakken van vijftien landen en twee internationale organisaties.
- *Big data, privacy en veiligheid* (2016-2017) – diverse policy briefings, rapporten, verkenningen en working papers, waaronder het rapport *Big Data in een vrije en veilige samenleving* (28 april 2016) waarin de WRR analyseert hoe de Nederlandse overheid Big Data kan gebruiken, specifiek gericht op het veiligheidsdomein. Big Data kan volgens de raad uitsluitend vruchten afwerpen als de huidige wet- en regelgeving wordt versterkt om fundamentele rechten en vrijheden te waarborgen.
- *De publieke kern van het internet. Naar een buitenlands internetbeleid* (maart 2015) – het internet dient een speerpunt te zijn van het Nederlandse buitenlands beleid. Dit is nodig om de publieke kern van het internet te vrijwaren van oneigenlijke interventies.
- *iOverheid* (15 maart 2011) – in het rapport doet de WRR een aantal aanbevelingen om het besef een iOverheid te zijn te verankeren in het beleid. Dit besef is van belang om de uitdagingen van de verdergaande digitalisering het hoofd te bieden.
- *ICT en internet* (4 oktober 2007) – deze studie beoogt de patronen van (on)veiligheid en van veiligheidszorg op het terrein van ICT en internet zo goed mogelijk te diagnosticeren (bijbehorende achtergrondstudie van het rapport *Onzekere veiligheid*).

KNAW

- *Hergebruik van publieke data* (december 2018) – publieke data van overheidsadministraties kunnen meer worden gebruikt en hergebruikt voor wetenschappelijk onderzoek.
- *Big data in wetenschappelijk onderzoek met gegevens over personen* (april 2018) – big data over personen biedt de wetenschap ongekende mogelijkheden voor nieuw onderzoek, maar stelt ook nieuwe eisen aan wetenschappelijke onderzoekers, die hun vraagstelling, en methoden en technieken opnieuw moeten bezien.
- *Ethische en juridische aspecten van informaticaonderzoek* (september 2016) – advies om voor informaticaonderzoek ethische beoordelingscommissies in te stellen.

VSNU

- *Versnellingsplan onderwijsinnovatie met ICT* (mei 2018) – plan gepresenteerd door de Vereniging van Universiteiten, Vereniging Hogescholen en SURF.
- *Digital Society Research Agenda* (november 2017) – leading the way through cooperation in a Digital Society.
- *Digitalisering in universitair onderwijs* (september 2017) – agenda voor een toekomstbestendig onderwijsaanbod.
- *Toekomstvisie De digitale samenleving* (september 2016) – Nederland en zijn universiteiten: internationale pioniers in mensgerichte informatietechnologie.

Raad van State

- *Ongevraagd advies over de effecten van de digitalisering voor de rechtsstatelijke verhoudingen* (31 augustus 2018) – digitalisering biedt de samenleving veel voordelen en kansen. Bij digitaal communiceren door de overheid staat het gemak van het functioneren van de overheid voorop. Overheidsorganen staan onvoldoende stil bij de gevolgen daarvan voor de verhoudingen tussen overheid en burger.

Raad voor het Openbaar Bestuur

- *Democratie, digitalisering en waarheid* (voorjaar 2020) – de bundel stelt de vraag centraal hoe in het digitale tijdperk waarheidsvinding gewaarborgd dient te worden in de democratie.
- *Zoeken naar waarheid. Over waarheidsvinding in de democratie in het digitale tijdperk* (9 mei 2019) – een analyse van de kansen en gevaren van digitalisering en formulering van een handelingsperspectief. De Raad noemt drie digitale beproevingen en benoemt voor de waarborging van waarheidsvinding vijf strategieën.
- *#WOEST. De kracht van verontwaardiging* (5 mei 2018) – de Raad verkent hoe de overheid het beste om kan gaan met de verontwaardiging van burgers en het grensoverschrijdend gedrag dat daar mogelijk het gevolg van is.
- *Van wie is deze hond? Politieke sturing op dienstverlening en ICT* (12 juni 2013) – de Tweede Kamer kan haar greep versterken op de rol die ICT speelt bij dienstverlening aan burgers. Volgens de Raad moet de Tweede Kamer zich in een vroegtijdig stadium buigen over het belang van ICT en dienstverlening in wetgevingstrajecten.
- *Gij zult openbaar maken. Naar een volwassen omgang met overheidsinformatie* (17 september 2012) – in het advies staat de vraag centraal op welke wijze openbaarheid van bestuur kan bijdragen aan de legitimiteit van en het vertrouwen in het openbaar bestuur.
- *Informatie: grondstof met toekomstwaarde* (20 maart 2008) – goede informatievoorziening ligt aan de basis van goed openbaar bestuur en de rechtstaat. Volgens de Raad schiet de overheid, door de voortschrijdende digitalisering, structureel tekort.
- *ICT en het recht om anoniem te zijn* (1 januari 2000) – de Raad probeert de vraag hoe de overheid moet omgaan met ICT-ontwikkelingen in relatie tot privacy en wie verantwoordelijk is voor de bescherming van de privacy, te beantwoorden.
- *Dienen en verdienen met ICT. Over toekomstige mogelijkheden van publieke dienstverlening* (1 april 1998) – de vraagstelling in het rapport is tweeledig: op welke beleidsterreinen veranderen de mogelijkheden tot ordening en zorg van de overheden en welk beleid is gewenst om de sociale cohesie te versterken?

De Nationale Ombudsman

- *Ombudsvisie op digitalisering overheid* (7 december 2017) – de ombudsman hield in eerdere rapporten de overheid een spiegel voor over de gevolgen van digitalisering. Hierin deed hij aanbevelingen

voor de digitale overheid. Op basis van deze rapporten heeft de Nationale Ombudsman vier uitgangspunten van belang geformuleerd.

TNO

- *Handvest 5G: samen op weg naar hoogwaardige digitale connectiviteit* (2019) – samen anticiperen op de hoge eisen die de technologische ontwikkeling van 5G stelt, is een van de meest vitale zaken voor de toekomst en zal grote invloed hebben op zowel burgers, bedrijven als overheden.
- *Gezond, veilig en kansrijk opgroeien* (2019) – dit rapport toont dat digitalisering kansen biedt om ervoor te zorgen dat alle kinderen gezond, veilig en kansrijk opgroeien.
- *We hebben deugden nodig voor ethische algoritmes* (2019) – dit artikel bespreekt algoritmes en artificiële intelligentie in overheid en openbaar bestuur.

Den Haag Centrum voor Strategische Studies (HCSS)

- *Hybrid Conflict: Neither war, nor peace* (10 januari 2020) – this Global Security Pulse examines trends within hybrid conflicts. The principal conclusion of this Pulse is that the international security environment is increasingly subject to hybrid threats, often in a subtle and pervasive way that impedes fast detection, accountability and retaliation.
- *Conflict in Cyberspace: Parsing the threats and the state of international order in cyberspace* (19 november 2019) – the Global Security Pulse on Conflict in Cyberspace was published in June 2019 and tracked emerging trends in relation to peace and security in cyberspace. This complementary research report delves into the two trend tables presented in the GSP by examining their underlying quantitative and qualitative evidence.
- *A balance of power in cyberspace* (15 juni 2018) – this article appropriates a realist model in international relations and adjusts it with neoliberal concepts of power to help better understand the challenge of stability between states in and on cyberspace.
- *Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks* (23 mei 2018) – this study examines the impact of cyber-related threats and challenges on corporate Europe and the degree of engagement of European business in tackling issues at stake.
- *Artificial Intelligence and the Future of Defense* (17 mei 2017) – the report contains an overview of the role that ‘intelligence’ – the computational part of the ability to achieve goals in the world – has played in defense and security throughout human history with a primer on AI.
- *Enabling big data applications for security: responsible by design* (17 maart 2017) – this report provides a description of technological developments and explains how these developments can be used to support more responsible, effective and efficient security.
- *Dutch Investments in ICT and Cybersecurity* (8 maart 2017) – this report provides a holistic overview of the current level of public and private investments in cybersecurity, followed by an analysis estimating the Dutch cybersecurity market by comparing different studies.

ECP – Platform voor de InformatieSamenleving

- *Artificial Intelligence en mensenrechten* (2019) – hoe ethische kaders elkaar versterken. In dit essay betogen we dat een ethische kader voor een verantwoorde toepassing van Artificial Intelligence en (mensen)rechten niet tegenover elkaar staan, maar juist in dienst staan van elkaar.
- *Aanpak begeleidingsethiek* (2019) – deze publicatie introduceert een aanpak voor het vruchtbaar verbinden van ethiek en innovatie.
- *Toezicht met algoritmen: Vinger aan de pols, werk aan de winkel* (2019) – praktijkanalyse voor evenwichtige inbedding van AI in de beroepspraktijk van toezichhouders.

- *Digitalisering Zorg & Privacy* (november 2018) – de toepassing van een dialoogmodel op portalen in de langdurige zorg.
- *Het verhaal van digitaal* (november 2018) – samen vormgeven van onze digitale samenleving. Het rapport gaat in op technologie, domeinen en digitale randvoorwaarden waarbij AI, de zorg en digitale vaardigheden extra uitgelicht worden.
- *White paper Artificial Intelligence* (2018) – gespreksstof en handvatten voor een evenwichtige inbedding in de samenleving.

Open State Foundation

- *Onderzoek naar register van verwerkingen* (juni 2019) – een onderzoek naar het register van verwerkingen bij gemeenten en provincies. Het doel van het onderzoek is om inzichtelijk te krijgen hoe gemeenten, provincies en ministeries zich houden aan artikel 30 van de Algemene Verordening Gegevensbescherming.
- *AVG-privacyregisters van de overheid slecht toegankelijk* (juni 2019) – artikel verschenen naar aanleiding van het onderzoek.

De Waag – technology & society

- *Datasamenleving & Democratie* (15 mei 2019) – rondetafelgesprek over de publieke waarden van technologische ontwikkeling. Privacy en (data)veiligheid zijn bekende issues, maar het gaat ook om zeggenschap over wie wij eigenlijk willen zijn. Om een betrouwbare, weerbare en democratische informatiesamenleving te bereiken zijn nieuwe, participatieve vormen van ontwikkeling en technologische governance nodig.

Adviesbureau Berenschot

- *Rapport Datagedreven sturing bij gemeenten samen aanpakken* (14 februari 2018) – onderzoek in opdracht van de Vereniging Nederlandse Gemeenten. Het rapport concludeert dat gemeenten veel aan elkaar kunnen hebben bij het veiliger en in de volle breedte van de organisatie invoeren van datagedreven sturing.

Wetenschappelijke bureaus politieke partijen

- Hans van Mierlo Stichting, *Robotisering in goede banen* (18 juli 2019) – deze publicatie onderzoekt de veranderingen op de arbeidsmarkt door robottechnologie. Deze transitie maakt ons bewust van nieuwe ongelijkheidsvraagstukken.
- Bureau de Helling, *Handvest voor de Slimme Stad* (november 2019) – technologie sturen op basis van waarden. Deze bundel presenteert een handvest voor smart cities waarin waarden als democratie, verbondenheid, menselijke waardigheid, privacy, duurzaamheid en gelijkheid vooropgesteld worden.
- Teldersstichting, *Digitalisering en Bildung* (2017) – de vierde dimensie van onderwijs. Dit onderzoek gaat over de dragers van het onderwijs: de docenten en hun hulpmiddelen, die in toenemende mate digitaal of virtueel van aard zijn.
- Wetenschappelijk Instituut voor het CDA, *Mens-zijn in de digitale samenleving* (november 2019) – perspectief op technologisch burgerschap. Digitale technologie is letterlijk een verlengstuk van onszelf geworden, maar hoe zorgen we ervoor dat de mens niet wordt gereduceerd tot een technisch subject of een digitaal profiel?

