# De Digitale D66 Agenda 2020-2030.

D66

# De Digitale D66 Agenda 2020-2030.

## Woord vooraf: digitale dilemma's verdienen politieke prioriteit

In het afgelopen decennium is digitalisering uitgegroeid tot een serieus politiek thema. Na de introductie van het internet in de vorige eeuw reageerden politici aanvankelijk enthousiast en hielden ze gepaste afstand. Later kregen ze oog voor de keerzijden van digitalisering en dataficatie maar bleven ze lang passief vanwege het complexe, ongrijpbare, private en grensoverschrijdende karakter ervan.

Inmiddels is niet alleen duidelijk dat digitale technologieën vergaande invloed hebben op maatschappelijke verhoudingen en burgerrechten, maar doen politici steeds serieuzere pogingen om digitalisering aan te jagen, bij te sturen en te begrenzen. Digitalisering raakt kernwaarden als vrijheid, gelijkheid en verbondenheid in het hart. Digitalisering is een politiek thema. Nu het eindelijk op die politieke agenda staat, moeten we concrete stappen zetten om de vele aspecten en verschillende dimensies van digitalisering in goede banen te leiden. Zodat alle mensen profiteren. Zodat menselijke autonomie en persoonlijke keuzevrijheid gewaarborgd blijven. Zodat Europa een kansrijke positie behoudt in de wereld. Zodat we de nationale veiligheid kunnen waarborgen. Oftewel: zodat de digitale samenleving van de toekomst humaan blijft.

Bij deze opdracht is het nodig een scherp oog te tonen voor de digitale dilemma's die op ons pad liggen. Deze vormen de kern van de politieke discussie van de komende jaren. De zes belangrijkste:

1. **Overheidscontrole versus burgervrijheid.** Hoe ver mag de overheid gaan in het verzamelen van persoonsgegevens om mensen in de gaten te houden?
2. **Commercie versus privac**y. Hoe ver mogen techbedrijven gaan in het verzamelen van persoonsgegevens om geld te verdienen?

3. **Staatscensuur versus tech-censuur**. Hoe beperken we de toenemende hoeveelheid ontwrichtende desinformatie zonder te vervallen in censuur?
4. **Internationaal concurrentievermogen versus nationale veiligheid.** In hoeverre laten we externe leveranciers een bijdrage leveren aan binnenlandse digitale infrastructuur?
5. **Opsporingsbelangen versus vitale infrastructuur.** In hoeverre mogen overheidsinstanties gebruik maken van softwarefouten die ook kwaadwillenden kunnen gebruiken?
6. **Verdienen versus verdelen.** Hoe voorkomen we een (verdergaande) digitale tweedeling in de samenleving als gevolg van robotisering, automatisering en algoritmes?

Met deze dilemma's in het achterhoofd heeft D66 voor de komende tien jaar een digitale agenda bestaande uit tien actielijnen[1], verdeeld over drie hoofdterreinen: **digitale vrijheid, digitale veiligheid en digitale verbondenheid**. Digitale ontwikkelingen gaan snel, we kunnen het ons niet langer veroorloven om dit voor ons uit te schuiven. Deze agenda vraagt tot slot om een betere **digitale organisatie**. D66 roept het huidige kabinet daarom op om in haar laatste maanden een begin te maken met de uitvoering van deze agenda, zodat het volgende kabinet hier meteen meters op kan maken. Dit is niet veel gevraagd en het geeft een hoop tijdwinst.

# I - Digitale vrijheid: Datasoberheid en publieke tegenmacht

Digitalisering in het algemeen en big data plus algoritmes in het bijzonder, bieden gigantische kansen op het gebied van energiebesparing, onderwijsverbetering, zorgkwaliteit en publieke dienstverlening. Grote vooruitgang ligt in het verschiet. Maar we mogen onze ogen niet langer sluiten voor keerzijden zoals het feit dat zowel overheden als grote bedrijven steeds meer data verzamelen, combineren en verwerken. Steeds vaker en vergaand met behulp van kunstmatige intelligentie.

Nadat de internetzeepbel begin dit millennium barstte, waren het de Amerikaanse techbedrijven die een nieuw verdienmodel ontwikkelden om de verwachtingen van de aandeelhouders waar te maken. Data werden het nieuwe goud of de digitale olie en de politiek stond erbij en keek ernaar[2]. Na privacy-schendingen in het eerste decennium van deze eeuw, kreeg het verdienmodel op basis van advertenties de afgelopen jaren steeds perversere trekken. Het doel van megapoortwachters zoals Google, Facebook en Twitter is om mensen zo lang mogelijk op hun platform te houden en de advertenties zo nauwkeurig mogelijk te laten aansluiten op de gebruiker. Dit gebeurt via *profiling* en *microtargetting*. Dat de content –in de vorm van desinformatie- hierbij niet zelden misleidend, intimiderend, discriminerend en polariserend is, wordt dan vaak bestempeld als: ‘niet onze verantwoordelijkheid’.

In plaats van ingrijpen, kopieerden overheden dit datamodel naar hun eigen werkwijzen en doelstellingen, zoals het bestrijden van onwenselijke zaken waaronder criminaliteit, fraude, terrorisme, kinderporno en pandemieën als Corona. De paradox hierbij: uit angst dat burgers de wet overtreden, overtreden overheden zelf steeds vaker ethische grenzen en zelfs de wet. Voorbeelden zijn de lokale wildgroei aan besluitvormingsalgoritmes en gezichtsherkenningscamera’s maar ook de wetsovertredingen van politie, veiligheidsdiensten, defensie en de belastingdienst in

hun datazucht en controledrang[3]. Onder het mom van “het doel heiligt de middelen” tornt de overheid zelf aan principes van de democratische rechtsstaat zoals onschuldpresumptie, dataminimalisatie, doelbinding en proportionaliteit. Het mes snijdt dus aan twee kanten en het is nodig deze trend een halt toe te roepen. D66 wil dat het kabinet zich op de volgende drie actiepunten richt:

## 1. De data-overheid moet zich aan de wet houden

Het afgelopen jaar werd duidelijk op hoeveel manieren de overheid haar eigen wetten overtreedt: dataverzameling door Defensie om burgers te monitoren, algoritmeproeftuinen van de politie, het Systeem Risico-indicatie (SyRI) van het ministerie van Sociale Zaken en Werkgelegenheid[4], het Fraude Signaleringssysteem (FSV) van de Belastingdienst, politie-apps die niet voldoen aan de privacywet AVG noch aan informatieveiligheid, onrechtmatige gegevensuitwisseling tussen het COA en de politie en de inlichtingendiensten die verkeerd omgaan met het verzamelen en bewaren van bulkgegevens. Dit datagedrag tast niet alleen ons grondwettelijke recht op privacybescherming aan. Het probleem is groter: als de wetshandhavers zelf ongestoord de wet kunnen overtreden, beschadigt dit onze democratische rechtsstaat en verslechtert de positie van de burger.

Er komt maar geen einde aan de datahonger van de overheid. Het kabinet wil nu vier grote samenwerkingsverbanden van tientallen organisaties de mogelijkheid geven onderling data uit te wisselen, samen te verwerken en aan derden te verstrekken: de Wet Gegevenssamenwerking Samenwerkingsverbanden(WGS). Effectief toezicht en handhaving door de Autoriteit Persoonsgegevens is echter vrijwel niet mogelijk door een gigantisch gebrek aan mankracht en middelen.[5] Dit probleem komt vaker terug bij de bescherming van persoonsgegevens, toezicht op algoritmes en het indammen van techreuzen.

- De overheid moet zich aan de wet houden. Dit is een basisprincipe.
- De overheid moet beter onderbouwen waarom ze data wil verzamelen, de hoeveelheid data zoveel mogelijk beperken, de data doelgericht gebruiken, transparanter zijn over de verwerking van data en data na gebruik vernietigen.

- Geef elke burger een digitale datakluis waarin persoonlijke gegevens als adres, leeftijd, en huwelijkse staat zijn opgeslagen. Burgers beheren deze kluis, overheden kunnen gegevens enkel -met toestemming- aan deze databron onttrekken[6]
- Toezichthouders als de Autoriteit Persoonsgegevens en het College voor de Bescherming van de Rechten van de Mens moeten meer mankracht en middelen krijgen.

## 2. Terughoudend gebruik van algoritmes en gezichtsherkenning

Zowel de overheid als het bedrijfsleven experimenteren op grote schaal met nieuwe technologie. Deze (vaak onzichtbare) wildgroei vindt plaats zonder breed maatschappelijk debat, duidelijke richtlijnen of wettelijke waarborgen. Reclassering deed recidive voorspellingen op basis van postcode gekoppeld aan criminaliteitscijfers in de buurt. De politie experimenteert in Roermond met algoritmes op basis van kenmerken als etniciteit en nationaliteit. Of deelt gratis deurbellen met camera's uit in gemeenten. In Rotterdam gebruikte de politie auto-camera's tegen Corona-overtredingen. En in Alphen aan de Rijn hing de Jumbo een gezichtsherkenningscamera op. Vaak is onduidelijk waar alle data uit camera's, sensoren of slimme flitspalen terecht komen en wat daar precies mee gebeurt.[7] Terughoudendheid en zorgvuldigheid is geboden maar in de praktijk is daadkracht en haast vaak leidend. In plaats van privacy-by-design, zien we overheden en bedrijven liever uitpakken met 'smart city' systemen. Oftewel: vrijwel ongeremde dataverzameling in de openbare ruimte.

Algoritmes hebben vergaande gevolgen voor grondrechten zoals non-discriminatie, sociale rechten en toegang tot het recht. Er is geen bewindspersoon verantwoordelijk voor ingrijpende algoritmes. Dit ligt verspreid over de ministeries van Economische Zaken en Klimaat, Justitie en Veiligheid, en Binnenlandse Zaken. Het gevolg is een oerwoud aan richtlijnen, ethische kaders, impact assessments en normen, terwijl de overheid tegelijkertijd erkent geen overzicht te hebben van welke ingrijpende algoritmische data-analyses die überhaupt in gebruik zijn door de Rijksoverheid.[8] Vanwege deze datapraktijk sorteren wettelijke waarborgen en onafhankelijk toezicht

onvoldoende effect. De datatrein dendert ongehinderd door. De minister voor rechtsbescherming erkende daarbij dat het voor mensen niet meer mogelijk is om zelflerende algoritmes te doorgronden.[9] Als de overheid niet in staat is om consistente en controleerbare besluiten over ingrijpende vraagstukken (uitkeringen, verdenkingen) te nemen, dan moeten zelflerende algoritmes in deze gevallen niet gebruikt worden.

- Het gebruik van algoritmes moet ethisch gebeuren. De ethische richtlijnen voor kunstmatige intelligentie van de High-Level Expert Group van de Europese Unie zijn zeer concreet. De Nederlandse overheid moet deze ten alle tijde toepassen[10].
- Het is tijd voor een Algoritme Autoriteit, die effectief toezicht kan houden op het gebruik van algoritmes.[11] Met steun van de Tweede Kamer heeft D66 het kabinet recent opgeroepen om vier toezichthouders een gezamenlijk onderzoek te laten doen naar de maatschappelijke gevolgen van algoritmes[12]. Dit is een eerste stap.

## 3. De overheid moet techreuzen tegenmacht bieden.

Elke macht heeft tegenmacht nodig. Elke markt heeft een strenge marktmeester nodig om te voorkomen dat een enkel bedrijf de dienst uitmaakt. De datamacht van de techreuzen Facebook, Google en Apple biedt hen een haast onoverbrugbare voorsprong. Elke byte aan informatie maakt het algoritme steeds slimmer. Uitdagers, startups en kleine concurrenten met minder data kunnen nooit zulke effectieve algoritmes maken. Zo sluit datamacht tegenmacht door uitdagers haast volledig uit. Daarbij bieden Facebook, Google en Apple een grote verscheidenheid aan diensten aan. Verschillende diensten van een enkel bedrijf kunnen moeiteloos data uitwisselen en als poortwachter bepalen ze wie toegang heeft tegen welke prijs. In Duitsland is het Facebook daarom verboden om data van Duitse burgers uit Facebook, WhatsApp en Instagram te combineren. Maar toezichthouders konden niet voorkomen dat Facebook voor 21.8 miljard dollar WhatsApp overnam. Dit omdat WhatsApp gratis is en nauwelijks omzet maakte. Een ouderwetse regel, die ervoor zorgt dat onafhankelijke mededingingsautoriteiten, zoals de Nederlandse Autoriteit Consument & Markt (ACM) onvoldoende tegenmacht kunnen bieden. Daarom moet het mededingingsrecht op onderdelen worden aangepast.[13]

Dat tegenmacht hard nodig is, blijkt uit het gedrag dat de techreuzen zich permitteren. Naast misbruik van marktmacht (waarvoor ze de boetes schouderophalend incasseren) en het schenden van privacy, onderbetalen ze veel personeelsleden en kleine makers die creatieve content creëren. Ook laten ze desinformatie, complotten en deepfakes vrijelijk op hun platforms woekeren totdat bedrijven of overheden aangeven dat het niet langer kan. Zo ondermijnen de techreuzen onze democratie, samenleving en economie.

- Ter bescherming van innovatie en concurrentie moeten techreuzen opgesplitst kunnen worden via het mededingingsrecht. Ook moeten marktmeesters fusies scherper onderzoeken, er voorwaarden aan verbinden en ze desnoods kunnen verbieden.
- Door techreuzen te verplichten hun data openbaar te maken, doorbreken we datamonopolies, opdat nieuwe bedrijven hun eigen algoritmes even slim kunnen maken.
- Het moet voor consumenten makkelijker worden om met hun eigen data over te stappen van techbedrijf naar techbedrijf (dataportabiliteit). Technische barrières moeten verdwijnen zodat alle aanbieders met hun diensten kunnen inbreken bij de dominante spelers (interoperabiliteit). Diensten van concurrenten mogen niet worden benadeeld op het eigen platform (non-discriminatie).

# II - Digitale veiligheid: Overwogen keuzes en Europese krachtenbundeling.

Technologie is een dominante factor in de mondiale verhoudingen. Wie de technologie bezit, zet de toon en bepaalt de standaard. Na de Amerikaanse tech-hegemonie, is China erin geslaagd een technologische wereldspeler te worden. Het is geen geheim dat Xi Jinping en de Communistische staatspartij de ambitie hebben rond 2030 het machtigste land ter wereld te worden, met technologie als voornaamste instrument. Cyberaanvallen en industriële spionage via achterdeurtjes worden daarbij niet geschuwd. Ingeklemd tussen deze twee machtsblokken zal een assertiever Europa een minder afhankelijke positie moeten creëren, in de vorm van een eigen tech-industrie, gezamenlijk cybersecuritybeleid en collectieve markteisen. Concreet betekent dit het stimuleren van Europese techbedrijven en een Europese Commissie die strengere voorwaarden stelt aan buitenlandse spelers die de Europese interne markt opkomen.

Intussen probeert een land als Rusland westerse democratieën te ontwrichten via desinformatie en digitale beïnvloeding. Technologische hulpmiddelen en digitale structuren zijn de nieuwe snelwegen om landen te bereiken en te ontwrichten. De overheid staat voor de taak om de vitale infrastructuur (elektriciteit, betaalverkeer, waterwerken, ziekenhuizen) te beschermen. Na jaren van druppels op gloeiende platen vergt dit een ambitieus Deltaplan, met als kern extra investeringen en een slagvaardigere organisatie. Nu is er te weinig geld en werkt de overheid te bureaucratisch. Daarbij moeten defensie, politie en de inlichtingendiensten kunnen beschikken over voldoende slagkracht en cyberwapens om Nederland te beschermen tegen binnenlandse criminelen en buitenlandse bedreigingen. Maar wel zonder dat dit leidt tot nieuwe cyberaanvallen als Wannacry en (Not)Petya waarbij niet gedichte softwaregaten het startpunt vormden[14].

## 4. Encryptie als principe en een zorgvuldige praktijk met zerodays

Encryptie maakt het mogelijk om informatie veilig te bewaren en berichten te versleutelen, zodat enkel afzender en ontvanger toegang tot de informatie hebben (end-to-end-encryptie, E2EE). Dit is belangrijk omdat mensen dan vrij kunnen communiceren zonder mogelijke tussenkomst van derden. Encryptie ligt onder vuur van politici en opsporingsdiensten, die uit controle-overwegingen graag mee willen kijken in de communicatie van burgers. Zij stellen hiertoe 'technische oplossingen' voor, zoals het inbouwen van verzwakkingen of achterdeuren in de versleuteling. Zulke achterdeuren worden echter niet enkel gebruikt door opsporingsdiensten maar ook door criminelen of kwaadwillende buitenlandse inlichtingendiensten. Door encryptie te verzwakken verliezen advocaten, journalisten, mensenrechtenactivisten en andere burgers een veilige manier om vertrouwelijk te communiceren.

We brengen onze samenleving ook in gevaar als we het gebruik van zerodays - een onbekende kwetsbaarheid in software - door politie, defensie en inlichtingen- en veiligheidsdiensten ongelimiteerd toestaan. Zerodays worden gebruikt door overheidsinstanties voor het verzamelen van inlichtingen- of opsporingsinformatie. Echter, criminelen gebruiken deze lekken ook graag, zoals toen ransomware in 2017 de haven van Rotterdam platlegde. Daarom diende D66 eind 2018 het initiatiefwetsvoorstel "Zerodays afwegingsproces" in, zodat het gebruik van zerodays door veiligheidsdiensten in het opsporingsbelang wordt afgewogen tegen het risico voor de samenleving als zulke zwakke plekken niet snel gemeld en opgelost worden.[15] Criminelen opsporen is belangrijk, maar garanderen dat ziekenhuizen hun chemobehandelingen niet hoeven te onderbreken door een cyberaanval ook.

- Het kabinet mag niet tornen aan het Nederlandse standpunt dat uitgaat van versleutelde gesprekken en dus sterkte encryptie.
- Er moet een wettelijk afwegingskader komen dat zorgt voor een overwogen en verantwoord gebruik van zerodays door defensie, politie en veiligheidsdiensten.

## 5. De nationale vitale infrastructuur vraagt betere beveiliging

Het is de verantwoordelijkheid van de overheid om onze democratie, onze vitale infrastructuur, onze bedrijfsgeheimen en onze staatsveiligheid te beschermen. Dit zonder te vervallen in censuur, zonder onverantwoord gebruik van cyberwapens en zonder lukraak bedrijven uit bepaalde landen te weren. Recent schreef de Rekenkamer dat staatsgeheimen van Buitenlandse Zaken slecht beveiligd zijn. Hierdoor liggen sabotage, spionage en diefstal op de loer. Een jaar geleden werd een kwetsbaarheid in Citrix-software geconstateerd, dit leidde tot het volledig stilleggen van veelgebruikte thuiswerksoftware. En de Wetenschappelijke Raad voor het Regeringsbeleid (WWR) concludeerde in 2019 dat Nederland niet goed is voorbereid op digitale ontwrichting.[16] Digitale infrastructuur is van levensbelang, zoals bleek tijdens de grote 112-storing van vorig jaar.

Dat het kabinet zijn eigen zaakjes nog niet op orde heeft, werd pijnlijk duidelijk toen EZ-minister Kamp staatsgeheimen mailde via zijn Gmail-account en onlangs opnieuw toen Defensie-minister Bijleveld een foto met inlogadres en toegangscode voor een geheime EU-meeting twitterde. Cyberhygiëne blijft een aandachtspunt. Veruit de meeste aanvallen zijn niet hightech maar low-tech: phishing mails, zwakke wachtwoorden en andere menselijke fouten. Ook kan de samenwerking tussen bedrijven, wetenschap en overheid beter. Onderzoekers op het gebied van cybersecurity worden vaak niet gehoord en hackers krijgen te maken met boze reacties als ze laten zien waar het mis gaat. Bedrijven melden datalekken of cyberaanvallen niet altijd tijdig en het Nationaal Cybersecurity Centrum (NCSC) heeft niet voldoende bevoegdheden om in te grijpen. Terwijl het voorkomen van cyberaanvallen juist gebaat is bij krachtenbundeling en informatie-uitwisseling.

Een tweede aandachtspunt is het snelgroeiende Internet of Things (IoT). Het ‘internet der dingen’ is het geheel aan apparaten die via internetverbindingen met andere apparaten of systemen in contact staan en daarmee gegevens uitwisselen. Dit creëert nieuwe verantwoordelijkheden voor producenten. Gehackte apparaten in bijvoorbeeld woningen of logistieke systemen vormen een toenemend veiligheidsrisico. Voor individuele gebruikers, maar ook voor de maatschappij als geheel, bijvoorbeeld als

grote hoeveelheden gehackte apparaten ingezet worden voor DDoS-aanvallen op banken of overheidswebsites[17].

- D66 wil een Deltaplan Cyberveiligheid dat zorgt voor voldoende geld en een slagvaardige cyberveiligheidsorganisatie, met als belangrijkste taak het voortdurend scannen van de vitale infrastructuur op kwetsbaarheden en verouderde software.[18]
- De bevoegdheden van het Nationaal Cyber Security Centrum moeten worden uitgebreid, zodat het NCSC kan fungeren als digitale brandweercommandant met de nodige kennis, expertise en bevoegdheden.
- Zorg voor betere afstemming tussen AIVD, MIVD, NCTV, NCSC, CERT's en private partijen.
- D66 wil een Nationaal Technologie Kader voor alle buitenlandse leveranciers in de Nederlandse vitale infrastructuur, bestaande uit een risicoanalyse en een eisenpakket, zoals audits toestaan en broncodes vrijgeven.
- D66 pleit voor (Europese) minimumeisen voor IoT-producten en een marktverbod voor slecht beveiligde IoT-apparaten, voorafgegaan door een nationale aanpak via een keurmerk of certificering en een verstevigd aansprakelijkheidsrecht.[19]

## 6. Een Europese tech-industrie en een Europese cyberveiligheidsstrategie

Modernisering vraagt om cruciale –specifieke- technologieën die Nederland niet allemaal zelf maakt. Dit is hoe de –op wederzijdse afhankelijkheid gebaseerde- wereldhandel werkt. Maar een toenemende dreiging is dat in de buitenlandse hard- en software onvindbare achterdeurtjes kunnen worden ingebouwd, waardoor buitenlandse actoren meekijken of informatie wegsluizen[20]. Het –op magere gronden- weren van het Russische antivirus-bedrijf Kaspersky, de kopzorgen over Huawei als leverancier van 5G-onderdelen en het niet afgeven van een Chinese exportvergunning voor ASML laten zien hoe complex deze vraagstukken zijn, zeker gezien de kleine schaal en grote internationale afhankelijkheid van Nederland. Enkel met technologische nauwkeurigheid en Europese samenwerking is dit beheersbaar te houden.

Deze Europese aanpak leunt op twee pijlers: proactief en reactief. Proactief betekent dat Europa een zelfbewustere positie moet innemen ten opzichte van de protectionistische machtsblokken VS en China. In wereldranglijsten van de grootste techbedrijven of snelst groeiende internetbedrijven komt Europa amper voor. Hier moet verandering in komen door doelgericht Europees innovatie- en industriebeleid dat startups en scale-ups zowel interne speelruimte als externe bescherming tegen overnames geeft. We zien dat bijvoorbeeld China met hoge subsidies en/of door overnames tegen bedragen hoger dan de marktwaarde, veelbelovende Europese startups en scale-ups overneemt, waardoor kennis en ideeën verdwijnen. De reactieve pijler betekent dat Europa zijn gewilde interne markt moet benutten om meer controle uit te oefenen op leveranciers van zowel consumentenelektronica als hard- en software voor de digitale infrastructuur.

- Gezien de grensoverschrijdende karakteristiek en de mondiale verhoudingen is een Europese Technologie-Strategie met bijhorend industriebeleid nodig. Hierin benoemen we welke technologieën Europa in eigen hand moet houden en hoe we onze technologie-toppers beschermen.
- Na jaren van nationale wetgeving heeft de Europese privacywet AVG laten zien dat de EU collectieve eisen kan stellen aan buitenlandse spelers. De versnipperde 5G-aanpak laat zien dat het tijd is voor een gezamenlijke Europese strategie op het gebied van cyberveiligheid in de vorm van collectieve controle- en veiligheidseisen.
- De EU moet instrumenten ontwikkelen tegen onwenselijke buitenlandse inmenging op de interne markt. Door de omzetdrempel vallen veelbelovende startups en scale-ups nu niet onder de bescherming van het Europese Witboek buitenlandse subsidies op de interne markt.

# III - Digitale verbondenheid: Samen presteren, eerlijk delen.

Digitale technologieën bieden enorme kansen op vooruitgang en verbetering. Met kunstmatige intelligentie kunnen we het klimaatprobleem te lijf en met algoritmes kunnen we kankercellen sneller detecteren. Bij het benutten van deze kansen spelen bedrijven en de wetenschap de hoofdrol, maar de overheid is als regisseur onmisbaar in het bijeenbrengen van spelers en het creëren van een kansrijk speelveld. Dit vergt het omvormen van het sectoraal verkokerde innovatiebeleid naar een aanpak waarbij innovatieve regio's oplossingen vinden voor mondiale uitdagingen als de energietransitie, het voedseltekort, de digitale transformatie en de vergrijzing.

Intussen moeten we constateren dat zich nog steeds hardnekkige problemen voordoen bij de inzet van data-projecten en ICT-systemen. Het is haast een publieke traditie dat ICT-projecten uitlopen, duurder uitpakken en geregeld mislukken. Naast een overheid die weet wat ze wil en wat ze kan, is moderne publiek-private samenwerking nodig om tot betere resultaten te komen. We moeten ook meer recht doen aan het belangrijke werk van onderzoekers, journalisten en hackers die de vinger op de zere plek leggen.

Tot slot profiteert lang niet iedereen in gelijke mate van de opbrengsten van digitalisering. Door automatisering, algoritmisering en robotisering verliezen sommige mensen hun baan terwijl de eigenaren van bedrijven en machines steeds vermogender worden. Ook kunnen lang niet alle mensen even gemakkelijk gebruik maken van digitale diensten, websites en apps. Een digitale tweedeling ligt daarom op de loer. Het is een gemeenschappelijke opgave om dit te voorkomen. Zonder voldoende (om)scholingsmogelijkheden, ondersteuning en voldoende inkomenszekerheid is dit niet haalbaar. Samen digitaliseren betekent ook samen profiteren.

## 7. Startups, scale-ups en innovatief MKB de ruimte geven

Niet alleen trekken economische grootmachten als China en de VS met een assertieve technologiestrategie steeds meer macht naar zich toe, ook presteren concurrenten als Israël, Singapore, Zuid-Korea en enkele EU-lidstaten beter op het vlak van wetenschap, innovatie en valorisatie. Na jaren van kwakkelend topsectorenbeleid moet Nederland keuzes maken en scherper focussen op toekomstbepalende sleuteltechnologieën. Deze technieken bepalen het concurrentievermogen van de Nederlandse economie. Hierbij gaat het onder meer om kunstmatige intelligentie, fotonica, nanotechnologie en biotech. Hetzelfde geldt voor de digitale infrastructuur: om digitale snelweg naar, digitaal knooppunt in en digitale koploper van Europa te blijven, is meer overheidsregie nodig.

Waar innovatieve bedrijven, onderzoeksinstellingen en de overheid samenkomen, vindt de meeste innovatie plaats. Zoals Brainport Eindhoven, Foodvalley Wageningen, AI-capital Amsterdam en Health hub Utrecht bewijzen. Toch kan Nederland nog veel terreinwinst boeken. Onze universiteiten en onderzoeksinstellingen zijn van wereldniveau, maar te vaak wordt van beschikbare kennis nog niet optimaal gebruikgemaakt. Niet alle spelers (kennisinstellingen, praktijkopleidingen, multinationals, leveranciers, groeibedrijven) weten elkaar te vinden. Om van uitvindingen marktsuccessen te maken, moeten we de werking van onze ecosystemen verbeteren. Shanghai en Sillicon Valley zijn lichtende voorbeelden.

Innovatieve ondernemers maken het verschil. De ruim 7.000 Nederlandse startups en scale-ups ontwikkelen innovatieve oplossingen en brengen deze op de markt. Opleidingen en innovatieregelingen moeten beter aansluiten op de bijzondere eigenschappen van startups en scale-ups. Andere landen slagen hier momenteel beter in dan Nederland. Hierdoor dreigt de uitstroom van talent en een verzwakking van onze kennispositie in de wereld.

- Moderniseer het innovatiebeleid. Verleg de focus van ouderwetse bedrijfstakken naar innovatieve regio's waarin overheden, kennisinstellingen, multinationals, MKB-leveranciers en start/scale-ups de krachten bundelen en oplossingen vinden voor internationale uitdagingen
- Waar mogelijk kiezen voor open data en open science zodat het delen van kennis tot vermenigvuldiging van succes leidt.
- Nederland moet de toon zetten met uitmuntende studies en ruime uitstroom van studenten naar banen bij deze groeibedrijven. En zorgen dat Nederlandse opleidingen goed aansluiten op de nieuwe vaardigheden die nodig zijn.
- Zorg dat startups en scale-ups de juiste kennis en mankracht hebben. Laat ze bijvoorbeeld makkelijker talent uit het buitenland halen en hun personeel betalen in aandelen. Nu kan dat nog niet.
- Maak het fiscaal aantrekkelijk om te investeren in startups en scale-ups. Zorg dat institutionele partners kunnen en mogen investeren in startups en scale-ups. Daarbij moeten we gebruik maken van instrumenten die het risico van institutionele beleggers gedeeltelijk afdekken.

## 8. Breng ICT-projecten op orde via een integrale aanpak

Als ICT en overheid in een zin worden genoemd, denkt iedereen aan falende of uitgelopen projecten. Veel ICT-projecten waren te ambitieus, zoals de digitalisering bij de Rechtspraak (kosten: 200 miljoen euro), het ICT debacle van 65 miljoen euro bij de Nederlandse Voedsel- en Warenautoriteit (NVWA) of de omgevingswet waar extra ICT kosten mogelijk tientallen miljoenen bedragen. Sinds een parlementaire commissie onderzoek deed naar de ICT-mislukkingen ziet het Bureau ICT-toetsing (BIT) toe op ontwerp en ontwikkeling van IT-systemen door de overheid. Dit neemt  niet weg dat de afhankelijkheid van een beperkt aantal softwareleveranciers leidt tot een vendor lock-in met als gevolg uitlopende schema's en oplopende kosten.

Soms gaat het wel goed. Na een overhaaste en veel te optimistische start liet het ontwikkelproces rond de CoronaMelder zien hoe het ook kan. Experts uit verschillende vakgebieden kwamen samen om het Ministerie van Volksgezondheid te ondersteunen. Op televisie werden pitches gehouden voor verschillende concepten

en openbare broncodes konden direct gecontroleerd worden. Er moet vaker worden samengewerkt tussen enerzijds experts uit het vakgebied die een bijdrage willen leveren en anderzijds ministeries en overheidsinstellingen die experts de ruimte geven voor innovatie en flexibiliteit. Een voorbeeld hiervan is Code for NL, een Nederlandse community van developers en designers die samenwerken aan een succesvolle digitale transformatie van de overheid en samenleving.

- Het BIT moet een meer onafhankelijke positie ten opzichte van ministeries krijgen met een sterker mandaat om niet goed ingezette of ontspoorde ICT-projecten tijdig bij te sturen of te onderbreken.
- De aanbestedingen van de overheid moeten minder geclusterd worden uitgezet, zodat ook partijen met kleinere schaal, lagere omzet en specifieke kennis een kans krijgen op een overheidsopdracht
- Overheidssoftware moet zoveel mogelijk open source zijn zodat de afhankelijkheid van grote leveranciers afneemt en iedereen mee kan helpen met de verbetering van ICT-systemen
- Ethische hackers moeten niet vervolgd maar beloond worden wanneer zij kwetsbaarheden aan het licht brengen.

## 9. Zorg dat iedereen kan profiteren van digitale technologieën

Zonder in dystopische voorspellingen te willen vervallen, is de afgelopen tijd duidelijk geworden dat lang niet alle mensen profiteren van de technologische ontwikkelingen. Tijdens de industriële revolutie maakten de Luddieten dit al duidelijk toen zij de nieuwe weefmachines vernietigden om hun baan te behouden. Er zijn afgelopen decennia al vele banen en bedrijven verdwenen als gevolg van de digitalisering. Kodak werd Instagram, V&D werd Bol.com en de regionale krant werd Facebook. Ook postbodes, taxichauffeurs, beurshandelaren en reisagenten kunnen hierover meepraten. Dit vergt aanpassingsvermogen van mensen maar de overheid moet hier wel hulp bij bieden in de vorm van omscholing en ondersteuning. Ook moeten de opbrengsten van automatische besluitvorming en robots, die sneller en goedkoper taken uitvoeren, eerlijker verdeeld worden. De weigerachtigheid om belasting af te dragen en offers te brengen aan het verdienmodel, laat zien dat overheden nodig zijn om het verschil tussen arm en rijk aanvaardbaar te houden.

Daarnaast moeten overheden hun eigen diensten zodanig aanbieden dat alle burgers ze kunnen begrijpen en gebruiken. Soms vergt het waarborgen van de toegankelijkheid van het digitale domein ondersteuning, soms een niet-digitaal alternatief.

- Nederland moet in de Europese Unie blijven inzetten op de realisatie van een digitaks. Als een beperkt aantal lidstaten dit blijft blokkeren, moet Nederland in navolging van landen als het Verenigd Koninkrijk, Frankrijk, Spanje en Oostenrijk nationale stappen zetten.
- Door het coronavirus en de geleidelijke digitalisering moeten we nu anders denken over werk als enige bron van inkomen. Om de inkomensverschillen binnen de perken te houden, moet de stap naar een basisinkomen in gang gezet worden.
- Net als publieke gebouwen moet ook de publieke dienstverlening voor iedereen toegankelijk zijn. De overheid moet mensen op leeftijd of met een beperking tegemoet komen in de vorm van persoonlijke ondersteuning, langere reactietermijnen of papieren alternatieven[21].

# IV - Digitale organisatie: een passende besluitvormingsstructuur.

Het realiseren van deze agenda 2020-2030 vergt een serieuzere politieke organisatiestructuur. Het huidige politieke debat vindt verkokerd en versnipperd plaats waardoor meerdere Kamercommissies afzonderlijk debatteren over grote vraagstukken als big data, kunstmatige intelligentie en de aanleg van het 5G-netwerk. In combinatie met een kennisgebrek zorgt overhaaste en overmoedige besluitvorming voor slechte wetgeving zoals de cookiewet en het downloadverbod tien jaar terug al lieten zien. Maar de eerdergenoemde WGS of het wetsvoorstel om Telecombedrijven te verplichten de locatiegegevens van miljoenen Nederlanders aan het RIVM te geven laten zien dat dit gevaar nog niet is geweken. Het digitale decennium 2020-2030 moet daarom beginnen met een structurele digitale besluitvormingsstructuur in Den Haag.

### 10. Een vaste Kamercommissie en een Minister van Digitale Zaken

In de afgelopen regeerperiode zijn betekenisvolle stappen gezet maar we zijn er nog niet. Na een eigen onderzoek, inclusief een blik op voorbeeldlanden als Denemarken of Duitsland heeft de Tweede Kamer het voornemen een vaste Kamercommissie Digitale Zaken op te zetten[22]. Daarnaast coördineert het kabinet de grote digitale vraagstukken beter dan voorheen via regulier overleg tussen de ministeries Binnenlandse Zaken, Justitie en Veiligheid en Economische Zaken en Klimaat. Na de verkiezingen is het zaak deze politieke structuren te vervolmaken, zodat Nederland zelfbewuste stappen kan zetten naar een kansrijke en humane digitale toekomst.

- Voer na de verkiezingen de aanbevelingen uit van de tijdelijke Commissie Digitale Toekomst van de Tweede Kamer[23]. Stel na de verkiezingen van 2021 een vaste Kamercommissie Digitale Zaken in. En stel na de formatie een ministerie van Digitale Zaken in.

# Eindnoten

1 Onderdelen van deze agenda zijn mede gebaseerd op eerdere D66-publicaties: Techvisie 1.0, Techvisie 2.0, het pamflet Digitale Revolutie, het Aanvalsplan Desinformatie, de initiatiefnota Digitale Mededinging, de initiatiefnota IoT-apparaten, de initiatiefnota Online identiteit en regie op persoonsgegevens en de Initiatiefwet Zerodays zijn de voornaamste. Alle vindbaar op D66.nl.

2 In haar boek “The Big Nine” bespreekt Amy Webb de veanderende verhoudinen tussen Sillicon Valley (techbedrijven), Wall Street (aandeelhouders) en Capitoll Hill (de politiek)

3 Zoals aangetoond na onderzoek door organisaties als (respectievelijk) de CTIVD, Bits of Freedom, NRC Handelsblad en KPMG.

4 Inmiddels door de rechter verboden

5 Motie van de leden Van Beukering-Huijbregts en Verhoeven over de capaciteit bij de Autoriteit Persoonsgegevens, 26 november 2020

6 Initiatiefnota Middendorp/Verhoeven, 13 juli 2018: https://www.tweedekamer.nl/kamerstukken/detail?id=2018D39573

7 Motie van de leden Verhoeven en Van Dam over het wettelijk kader voor gezichtsherkenningstechnologie, 21 november 2019

8 Beantwoording vragen commissie over waarborgen tegen risico’s van data-analyses door de overheid, Kamerbrief, 20-05-2020

9 Kamerbrief over toepassing artificiële intelligentie en algoritmen in de rechtspraak, 19 december 2018.

10 Het gaat om deze richtlijnen: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

11 Motie van de leden Verhoeven en Van der Molen over een meldplicht voor ingrijpende algoritmes, 10 september 2019

12 Het gaat om de Autoriteit Persoonsgegevens, het College voor de Bescherming van de Rechten van de Mens, de Autoriteit Consument en Markt en de Algemene Rekenkamer.

13 Initiatiefnota van het lid Verhoeven over mededinging in de digitale economie, 5 februari 2019

14 Wannacry en (Not)Petya zijn twee cyberaanvallen in 2017 die misbruik maakten van de Eternalblue exploit die door de Amerikaanse veiligheidsdiensten werd ontwikkeld op basis van een onbekende kwetsbaarheid (zero-day). Door deze cyberaanvallen kregen vele landen te maken met grote verstoringen van vitale functies.

15 Initiatiefwet Verhoeven Zerodays Afwegingskader, 19 juli 2019: https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?id=2019Z15289&dossier=35257

16 https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting

17 DDoS staat voor Distributed Denial of Service. Bij dit soort aanvallen wordt een computer of website platgelegd door hem heel vaak in korte tijd vanaf verschillende computers te benaderen.

18 Motie van de leden Verhoeven en Laan-Geselschap over het op kwetsbaarheden scannen van overheidssystemen in de vitale infrastructuur, 25 juni 2019

19 Initiatiefnota van het lid Verhoeven: "Het Internet der Dingen: maak apparaten veilig!", 24 november 2016

20 Organisaties als de NCTV en de AIVD hebben hier in rapportages herhaaldelijk op gewezen.

21 Verkiezingen, ingrijpende besluiten en bepaalde overheidsdiensten kunnen pas digitaal als het veilig, betrouwbaar en voor iedereen beschikbaar is.

22 Dit lijkt een procedureel punt maar een vaste commissie is het aanspreekpunt voor burger- en brancheorganisaties en kan naast het voeren van hoofdlijndebatten ook het kabinet beter tot de orde roepen.

23 Zie het eindrapport "Update Vereist" van de tijdelijke commissie Digitale Toekomst: https://www.tweedekamer.nl/nieuws/persberichten/eindrapport-tijdelijke-commissie-digitale-toekomst-"update-vereist"