

Techvisie

D66



d66.nl/techvisie

Techvisie

D66

Kees Verhoeven

Marijn van Vliet

Nick Mastenbroek

Myrthe van Dieijen

Dick van Egmond

Ouke Arts

Inhoud

Samenvatting en belangrijkste aanbevelingen	6
Inleiding: technologie schept een nieuwe wereld	13
De dynamiek van nieuwe techniek	13
Het politieke debat ontbeert samenhang	15
Visie: De overheid in een digitaal tijdperk	16
Technologie en maatschappelijke dilemma's	17
Mens en overheid vanuit sociaal-liberaal perspectief	18
Verschillende rollen voor de overheid in het digitale domein	18
De visie van D66: Nederland in 2030	18
Hoofdstuk 1: De Internet economie	21
Visie 2030: Nederland als digitale koploper van Europa	22
Aanbevelingen	23
Maak radicaal ruimte voor vernieuwing...	23
...En help verliezers van vooruitgang mee vooruit (vrees robots niet!)	24
Fors meer investeren in onderzoek en innovatie	28
Maak investeren in startups aantrekkelijker	28
Benut de mogelijkheden van open data	30
Ontwikkel integraal beleid rond de derde mainport	31
Van Topsectoren naar maatschappelijke domeinen	31
Bewaak eerlijke concurrentie op het digitale speelveld	31
Kies voor echte Netneutraliteit	34
Zo snel mogelijk naar één Digitale Markt	34
Hervorm het intellectueel eigendom...	34
...En moderniseer het auteursrecht	35
Hoofdstuk 2: Technologie in het publieke domein	36
Visie 2030: technologie ondersteunt de mens	38
Aanbevelingen	39
Stimuleer de ontwikkeling van digitale vaardigheden	39
Stel de leerling centraal via digitaal onderwijs	40
Met robots naar menselijke zorg	41
Stel de patiënt centraal via technologie in de zorg	42
Geef patiënten inzicht in de zorgkwaliteit	43
Zet in op slimme steden maar blijf realistisch	43
Versterk de democratie door digitalisering	44
Experimenteer met digitale dienstverlening	45
Meer realisme en betere organisatie van ICT-projecten	46
Maak technologie tot kabinetsprioriteit	47

Hoofdstuk 3: Online vrijheid	49
Visie 2030: Een open en vrij internet dat niet stiekem ingrijpt in onze levens	51
Aanbevelingen	51
Geef dominante internetbedrijven een zorgplicht	51
Informeel gebruikers over de werking van algoritmes	54
Voorkom datadiscriminatie van consumenten	55
Geen data verzamelen zonder expliciete toestemming	56
Laat mensen hun gegevens inzien en waar nodig aanpassen of wissen	57
Meer budget en capaciteit Autoriteit Persoonsgegevens	57
Voorkom dat schijnveiligheid onze vrijheid inperkt	58
Encryptie als grondrecht	60
Laat als overheid zien welke data je verzamelt en gebruikt	61
Privacy by Design: beperk basisregistraties en bestandenkoppeling	62
Strijd wereldwijd voor een open en vrij internet	62
 Hoofdstuk 4: Digitale veiligheid	 64
Visie 2030: Nederland als Veilige haven en toevluchtsoord	65
Aanbevelingen	66
Aansprakelijkheid voor nalatigheid door slechte software	66
Bescherm onderzoekers en hackers	66
Kwetsbaarheden in software dichten en niet misbruiken	67
Veilig gebruik van drones, geen gebruik killerrobots	68
Een sterker en onafhankelijker NCSC	69
Werk samen met bedrijven op operationeel niveau	70
“Security by Design” en open source software als standaard	70
Een veilige infrastructuur in private handen	71
Veilige Digitale Authenticatie en Identificatie	72
Voer campagne vóór cyberhygiëne	73
 Financieel Overzicht	 75
 Verantwoording en geraadpleegde bronnen	 75

Samenvatting

en belangrijkste aanbevelingen

Technologische verandering heeft steeds meer maatschappelijke invloed

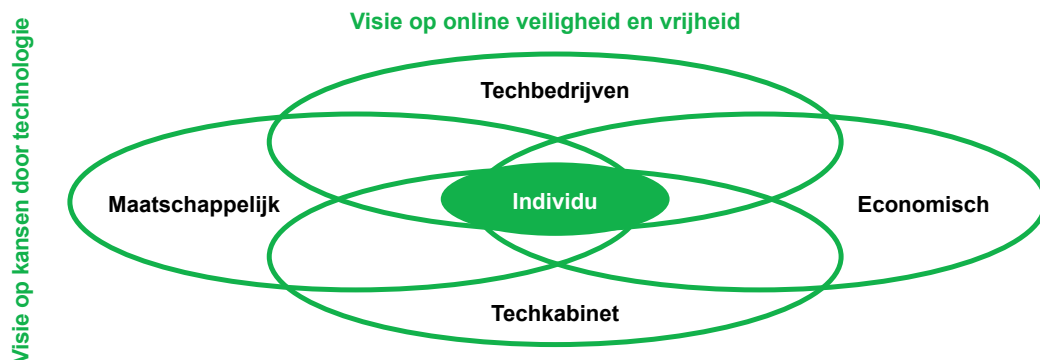
Technologie bepaalt en verandert ons leven en dat geldt zeker voor het internet. Privé zijn we continu online en op ons werk worden we omringd door ICT. Steeds meer apparaten worden de komende jaren aangesloten op het internet. 3D printen verandert het mondiale productiesysteem. En door Big Data komen gegevens beschikbaar die vroeger niemand kende. De voortschrijdende digitalisering beïnvloedt ook de organisatie van onze zorg, ons onderwijs en onze overheid.

Technologische veranderingen gaan steeds sneller en de maatschappelijke invloed is steeds groter. Zowel bij het benutten van kansen (economische groei, betere dienstverlening) als bij het bedwingen van bedreigingen (privacyschendingen, cybercrime), heeft de overheid een belangrijke rol. Dit vraagt om een samenhangende toekomstvisie. Maar het politieke debat bestaat nu vooral uit boze reacties op gehackte OV-chipkaarten, mislukte ICT-projecten of irritante cookiemeldingen.

De overheid heeft verschillende verantwoordelijkheden in het digitale domein

Net als in de fysieke wereld heeft de overheid ook in het digitale domein verschillende verantwoordelijkheden. Allereerst waarborgen dat nieuwe technieken, informatie en voorzieningen voor iedereen toegankelijk zijn. Ten tweede burgers en ondernemers beschermen tegen criminelen en machtige bedrijven. Maar –via onafhankelijk toezicht– ook tegen de overheid zelf. Ten derde ruimte geven aan initiatief en innovatie stimuleren. De overheid is dus zowel hoeder van een vrij en open internet, scheidsrechter tussen mensen en ondernemingen, verzamelaar van persoonsgegevens en inkoper van ICT-systemen. Met deze verschillende rollen en de spanningsvelden daartussen moet goed rekening gehouden worden.

Vandaar deze Techvisie. D66 stelt hierin niet de technologie of het internet zelf centraal maar de gevolgen ervan op vier centrale onderdelen van onze samenleving: vrijheid, veiligheid, de economie en het publieke domein. Vanuit een sociaalliberale invalshoek op mens en overheid doen we concrete aanbevelingen op elk van deze vier terreinen.



Nederland in 2030: digitale koploper en veilige datahaven

Het verleden heeft bewezen dat technologische ontwikkelingen de kwaliteit van leven vergroten. D66 omarmt vooruitgang en wil dat Nederland hierin voorop loopt. Het tegenhouden van verandering is een achterhoedegevecht waar niemand beter van wordt. Echter, naast meebewegen met de praktijk blijft ook het bewaken van principiële grenzen nodig. Dat iets kan, betekent niet automatisch dat het moet. Dat het technisch mogelijk is alles van iedereen te weten, wil niet zeggen dat het menselijk en wenselijk is.

Nederland was het tweede land ter wereld dat netneutraliteit wettelijk verankerde. We liepen voorop met de leidraad *responsible disclosure* om goedwillende hackers te beschermen. En het huidige kabinet zet zich in voor de digitale infrastructuur als derde mainport en voor sterke encryptie zonder achterdeurtjes. D66 streeft ernaar dat Nederland in 2030 de digitale koploper is van Europa. Een broedplaats, thuishaven en trekpleister voor innovatieve bedrijven en talentvolle individuen. Met inwoners die dankzij goede digitale vaardigheden grip hebben op digitale kansen en bedreigingen. Met bedrijven die digitale kansen benutten. Met een overheid die technologie omarmt en stimuleert. Ook is ons land in 2030 een veilige haven voor persoonsgegevens. Dankzij bewuste keuzes die mensen kunnen maken om zich te beschermen tegen publieke en private dataverzamelaars uit de hele wereld. Internationaal is Nederland een voorvechter van een vrij en veilig internet. Encryptie is een grondrecht en we zijn een toevluchtsoord voor goedwillende hackers. Het ingrijpen in internetprotocollen en het handelen in (onbekende) software-kwetsbaarheden (*zero day exploits*) wijzen we af. Anders dan de Amerikaanse overheid in de zaak Apple vs. FBI zet Nederland de veiligheid van het internet niet op het spel.

Belangrijkste aanbevelingen

1. Omarm technologie en stel de mens centraal

- Benut de kansen van automatisering. Robots en software kunnen steeds meer menselijke taken overnemen. Net als bij vorige industriële revoluties is dit voordelig mits mensen zich richten op datgene waar ze het beste in blijven: creativiteit, improvisatie en empathie. Snel inspelen op onvermijdelijke veranderingen is beter dan kansloze achterhoedegevechten voeren. Niet alleen in industrie en dienstverlening maar ook in de zorg (robots) en het onderwijs (online courses) liggen hier kansen.
- Nederland als technologisch laboratorium. De transportwereld en de inrichting van ons land zal onomkeerbaar veranderen door zelfrijdende auto's en drones. Blockchaintechnologie haalt de bank uit het betalingsverkeer en kan financiële fraude terugdringen. Super- en quantumcomputers gaan de rekenkracht verveelvoudigen. En met het internet der dingen worden 50 miljard apparaten op internet aangesloten. Nederland moet hierin investeren! Niet alleen financieel maar ook door voldoende testlocaties, moderne regelgeving en veilige infrastructuur.

- Geef kinderen al op de basisschool les in programmeren. Maak digitale vaardigheden niet alleen onderdeel van het curriculum van (basis)scholen maar ook van lerarenopleidingen. Besteed in het onderwijs tevens meer aandacht aan ondernemerschap, 3D-printen, Big Data en de risico's van social media.
- Ondersteun digitale achterblijvers. Niet iedereen profiteert tegelijk of evenveel van nieuwe technologie. De overheid moet benadeelden helpen en de voordelen van digitalisering zo eerlijk mogelijk verdelen. Dat vraagt doelgericht en levenslang onderwijs, het beschermen van werknemers en sociale vangnetten. Maar ook hulp bij digitale systemen. Dus niet krampachtig vasthouden aan de blauwe enveloppe maar wel helpen bij het online aangifte doen.
- Laat data ons leven makkelijker maken. Mits goed ontsloten kunnen data mensen helpen bij het maken van keuzes. Bij het kiezen van een zorgaanbieder of behandelmethode. Of persoonlijke leerbehoeftes. Voorwaarde is dat deze data zeer goed beveiligd zijn en dat alleen de eigenaar bepaalt wat ermee gebeurt.

2. Investeer fors in innovatie en de digitale economie

- Investeer €1 miljard extra in onderzoek en innovatie. Het verleden heeft bewezen dat publieke investeringen in onderzoek lonen. Maar Nederland raakt steeds verder verwijderd van de Lissabondoelstelling om 2020 1% BBP aan innovatie uit te geven. Om een substantiële stap te zetten, wil D66 hier richting 2020 €1 miljard extra voor uittrekken. Naast meer geld is ook een andere sturing nodig. Daarom moeten de negen topsectoren vervangen worden door maatschappelijke uitdagingen (zoals het grondstoffentekort of de vergrijzing) en veelbelovende technologieën.¹ Ook moet het fiscaal aantrekkelijker worden om in startups te investeren.
- Versterk de rol van de Autoriteit Consument en Markt (ACM) in het digitale domein. Eerlijke concurrentieverhoudingen zijn binnen het digitale speelveld allesbehalve vanzelfsprekend: de mondiale reikwijdte van diensten en de netwerkeffecten van platforms zorgen snel voor dominante spelers (Microsoft, Google, Facebook, Uber). De mededingingswet voldoet inhoudelijk maar de handhaving moet intensiever en doelgerichter. D66 wil het budget van de ACM vergroten zodat er een speciaal team digitale mededinging kan worden gevormd.
- Moderniseer het Intellectueel Eigendom en het auteursrecht. Patenten leiden steeds meer tot vergaande juridisering en steeds minder tot baanbrekende innovaties. Daarom wil D66 dat patenten beperkter worden uitgegeven (alleen bij echte doorbraken) sneller verlopen (*use it or lose it*) en makkelijker aanvechtbaar zijn. De 28 nationale auteursrechtstelsels moeten worden vervangen door één

¹ Zoals Duitsland doet met het Industrie 4.0 programma.

Europees auteursrecht (met Europese licenties) zoals eerder is gebeurd met het merkenrecht en contractrecht. Digitale grenzen binnen de EU (*Geo-blocking*) moeten zo snel mogelijk worden afgeschaft. Mensen moeten uitzending gemist ook in andere EU-lidstaten kunnen bekijken.

3. Versterk de positie van gebruikers ten opzichte van dominante internetbedrijven

- Leg internetreuzen net als banken een zorgplicht op. Hun nutsfunctie in combinatie met hun informatiemacht rechtvaardigt dit. Facebook weet bijna alles van zijn 1.7 miljard gebruikers (“privacy is dead; get over it.”²) en de zoekmachine van Google kan de Amerikaanse verkiezingen voor 25% beïnvloeden! Dit betekent onder meer: meer openheid over verzamelde persoonsgegevens, doelbinding beter respecteren, leesbare privacyvoorwaarden en actiever informeren over standaardinstellingen.
- Verdriedubbel het budget van de Autoriteit Persoonsgegevens (AP). Veel van het bovenstaande is in lijn met de Wet bescherming persoonsgegevens (Wbp) en het onlangs vastgestelde Europese dataproductiepakket.³ Maar de digitale praktijk is weerbarstig en het is moeilijk je recht te halen tegen almachtige internetbedrijven. Daarom moeten het toezicht en de handhaving strenger – Europees en nationaal. Het budget van de AP moet daarom van 8 naar 25 miljoen euro in 2020.
- Voorkom datadiscriminatie en laat de invloed van algoritmen zien. Vergelijkbaar met de bijsluiter van een medicijn. Online behandeling (de prijs van een vliegticket, de uitkomst van een zoekopdracht) wordt gebaseerd op onzichtbare rekenregels die persoonsgegevens vertalen naar profielen. Prijsdiscriminatie en informatiesturing staan op gespannen voet met de algemene wet gelijke behandeling. Bedrijven moeten consumenten actief informeren over deze onzichtbare algoritmes. Indien nodig dwingen we dit af via wetgeving.
- Bewaak online keuzevrijheid. Mensen moeten vrij kunnen kiezen uit online producten en diensten. Handhaving van de mededingingswet moet zo georganiseerd zijn dat grote diensten als Facebook en Google hun marktaandeel niet misbruiken. De Autoriteit Consument en Markt (ACM) moet hier meer middelen voor krijgen. Ook de keuze over *profiling* moet bewust zijn. De cookiewet is niet het goede antwoord op het heimelijk verzamelen van persoonsgegevens. Weloverwogen toestemming geven moet daarom via de browser geregeld worden.

2 Naar verluidt woorden van Facebook CEO Mark Zuckerberg.

3 Bestaande uit een Algemene Verordening Gegevensbescherming (AVG, voor publieke en private organisaties) en een Richtlijn Gegevensverwerking (omdat politie en justitie het domein van de lidstaten zijn, is dit een richtlijn met enige uitzonderingen, die landen met een eigen wet moeten implementeren).

- Garandeer gegevenscontrole. Verzamelde gegevens blijven eigendom van de gebruiker en mogen niet zomaar worden gedeeld of doorverkocht. De eigenaar moet de gegevens altijd kunnen inzien en aanpassen of wissen. Ook hier is de praktijk vaak anders dan het papier: dus zorg bij het recht om vergeten te worden voor snelle besluitvorming over het verwijderen van zoekresultaten.

4. Wees als overheid terughoudend met het verzamelen van data

- Voorkom dat schijnveiligheid persoonlijke vrijheden inperkt. Het kabinet heeft drie wetten in voorbereiding die bevoegdheden van inlichtingen- en opsporingsdiensten vergroten⁴. Begrijpelijk in tijden van terreur maar inhoudelijk problematisch. Allereerst omdat het niet werkt. Bill Binney, voormalig technologie directeur bij de Amerikaanse NSA zegt, “totalitarian mass surveillance will cost lives”. Ten tweede is het een inbreuk op fundamentele burgerrechten omdat iedere burger bij voorbaat als verdachte beschouwd wordt. Ten derde schaadt het de digitale economie omdat bedrijven hun klantdata in Nederland niet kunnen garanderen. In plaats van datasleepnetten, mass surveillance en hackende politieagenten wil D66 human intelligence, verplichte informatie-uitwisseling tussen nationale diensten, betere waarborgen en scherp toezicht achteraf. Het budget van de toezichthouder op de inlichtingendiensten (CTIVD) moet omhoog en er moet extra toezicht komen op de opsporingsdiensten, zeker als ook de politie –na het leger en de inlichtingendiensten- een hackbevoegdheid krijgt.
- Geef als overheid volledige inzage in de data die je verzamelt en gebruikt. Juist omdat de burger vaak verplicht is om deze gegevens te overleggen, moet voor burgers altijd duidelijk zijn welke gegevens bij de overheid bekend zijn en welke instantie ze gebruikt.⁵ Naast wettelijke inperking van de verzameldrift en versterking van het onafhankelijk toezicht hierop is het nodig de analyse en het gebruik van Big Data door de overheid strakker te reguleren.⁶
- Beperk het aantal basisregistraties en bestandkoppelingen. Heeft de overheid al die data eigenlijk wel nodig? Met liefst twaalf basisregistraties, talloze gekoppelde bestanden en een nieuw authenticatie-systeem dat standaard alle gegevens opvraagt, is dat zeer de vraag. Daarom moet de overheid werk maken van betere doelbinding en meer *privacy by design*, onder meer bij aanbestedingen en inkoop van hard- en software.

4 De wet computercriminaliteit III, de wet bewaarplicht en de wet op de inlichtingen- en veiligheidsdiensten (wiv).

5 Estland is hier heel ver mee via het programma X-road. Zowel inzien als corrigeren is mogelijk. Ook wordt strenger toegezien op misbruik van gegevens.

6 Zoals de WRR terecht adviseert in hun rapport “Big Data in een vrije en veilige samenleving” (2016)

5. Sta voor een vrij en veilig internet en draag dit internationaal uit

- Beschouw encryptie als het briefgeheim van de 21^e eeuw. Goede versleuteling beschermt persoonsgegevens, bedrijfsgeheimen en documenten van de overheid. Het maakt het internet veiliger en is daarmee ook van economisch belang. Nederland moet encryptie stimuleren en dit wereldwijd uitdragen. Dat betekent uiteraard ook dat Nederland geen offensief gebruik maakt van (nog onbekende) softwarefouten (*0 days, backdoors*) en dat de politie niet mag hacken via technische kwetsbaarheden, zoals het wetsvoorstel computercriminaliteit 3 regelt. Immers, dat zou de politie een motief geven om het internet te verzwakken: een weg die we niet op moeten.
- Sta pal voor internetvrijheid. Dat is nodig nu overheden het internet steeds meer willen controleren voor auteursrechtenbescherming, terreurbestrijding of burgercontrole. Nu landen steeds meer technische capaciteiten krijgen, moet Nederland zich internationaal verzetten tegen contentfilters, webblokkades en censuur.
- Leg wettelijk vast dat overheden niet ingrijpen in internetprotocollen. Steeds meer landen willen controle over hun burgers via het internet (via afscherming, blokkades, censuur, surveillance) en over het internet zelf (via netneutraliteit, het beheer en de uitgifte van namen en nummers).⁷ Steeds vaker raakt dit de centrale protocollen waarop het internet draait (Internet Protocol, Domain Name System Protocol, etc.). Dit maakt het internet onveiliger en onbetrouwbaarder. Daarom moet Nederland zich inzetten voor een internationale afspraak dat landen de centrale internetprotocollen met rust laten.
- Laat software onder garantie vallen. Alhoewel er een ISO-norm voor software is, is de aansprakelijkheid bij fouten of fraude vaak niet duidelijk. D66 wil dat bedrijven aansprakelijk gesteld kunnen worden voor slechte software. En dat software binnen een redelijke termijn onder een garantie valt zodat een consument zijn recht kan halen. Ook moet open source software de standaard zijn bij publieke inkoop en aanbestedingen.
- Maak het Nationaal Cyber Security Centrum (NCSC) onafhankelijk. Om de cyberveiligheid in Nederland nog beter te dienen, moet het NCSC echt onafhankelijk worden, vergelijkbaar met het Rijksinstituut voor Volksgezondheid en Milieu (RIVM). Zo kunnen justitie of de AIVD geen invloed uitoefenen op de adviezen. Ook goedwillende hackers moeten hun werk kunnen doen. Daarom wil D66 dat hackers die de leidraad Responsible Disclosure hebben gevolgd, nooit strafrechtelijk vervolgd kunnen worden.

7 De WRR noemt deze trend in hun rapport "De publieke kern van het internet" securitisation.

6. Maak technologie en internet tot prioriteit van het kabinetsbeleid

- Stel een minister van Economie, Technologie en Privacy aan. Deze aanjager van de digitale economie, bewaker van eerlijke concurrentie en hoeder van burgerrechten staat aan het hoofd van een nieuwe digitale driehoek voor technologie- en internetbeleid. Analoog aan de zeshoek⁸ die kabinetten vormen om het financiële en sociaaleconomische beleid te coördineren. Deze digitale driehoek moet verder bestaan uit de ministeries van Justitie (rechtstaat, opsporing en cybersecurity) en van Binnenlandse Zaken (inlichtingendiensten en ICT-inkoop). Deze drie ministeries worden geflankeerd door vijf sterke en onafhankelijke toezichthouders: de ACM (mededinging), de AP (persoonsgegevens), het NCSC (cybersecurity), de CTIVD (inlichtingendiensten) en het BIT (project-toetsing).
- Ontsluit alle overheidsdata als open data. Informatiebestanden die met belastinggeld zijn aangelegd moeten vrij toegankelijk zijn. Dit maakt niet alleen controle van de overheid makkelijker maar leidt ook tot innovaties (zoals Buienradar). Hetzelfde geldt voor semipublieke organisaties zoals het handelsregister van de Kamer van Koophandel. Omdat het vaak om verplicht aangeleverde gegevens gaat, moeten burgers te allen tijde tegen misbruik beschermd worden.
- Professionaliseer de inkoop en aanbesteding van ICT. D66 onderschrijft de adviezen van de tijdelijke commissie ICT-projecten. Maar de wijze waarop het kabinet het Bureau ICT-toetsing (BIT) heeft ingericht, is niet goed. Door het onder leiding van de CIO rijk te stellen, is onafhankelijke toetsing onmogelijk. Dit moet alsnog geregeld worden. Verder moet de ICT-kennis bij de Rijksoverheid snel worden verbeterd en moet stevast gekozen worden voor open source software. Zodat de afhankelijkheid van leveranciers afneemt. Ook moet de Nederlandse overheid –in navolging van het Verenigd Koninkrijk- meer inzetten op “lenige” softwareontwikkeling: in plaats van een vooraf vastomlijnd eindproduct kiezen voor een snel werkbaar product dat vervolgens wordt doorontwikkeld.

8 Bestaande uit de Minister-President en de ministers van Financiën, Sociale zaken, Economische Zaken, Binnenlandse Zaken en Volksgezondheid.

Financieel Overzicht

• Investeren in onderzoek en innovatie	€1 miljard
• Versterken positie Autoriteit Persoonsgegevens	€ 17 miljoen
• Versterken positie Autoriteit Consument & Markt	€ 6 miljoen
• Versterken positie CTIVD	
• Inclusief uitbreiding naar toezicht op opsporingsdiensten	€ 4 miljoen
• Onafhankelijk maken NCSC	€ 3,5 miljoen
• Betere campagne Cyber hygiëne	€ 0,5 miljoen

Inleiding: technologie schept een nieuwe wereld

De dynamiek van nieuwe techniek

Technologie bepaalt ons leven en dat geldt zeker voor het internet. We zijn online vanaf het moment dat we opstaan. Onze smartphones, tablets en computers staan centraal in het communiceren en het vinden van informatie. Op onze Xbox of Playstation gamen we met mensen over de hele wereld en dankzij Netflix en Spotify kunnen we overal series kijken of muziek luisteren.

Op ons werk zijn we omringd door ICT. De gemiddelde werknemer zit 4 uur per dag achter de PC.⁹ Voor ondernemers was het nooit zo makkelijk een idee te realiseren. Via websites als Freelancer.com kan een ondernemer programmeurs over de hele wereld vragen een website, app of software te ontwikkelen en die binnen een paar minuten online zetten dankzij cloud computing.

Ook publieke sectoren als onderwijs en zorg maken de digitale revolutie mee. Veel leerlingen kijken bij het studeren voor het eindexamen naar Youtube colleges. Studenten op de universiteit hebben de beschikking over tal van Massive Online Open Courses (MOOC's) van prestigieuze universiteiten als Harvard en Cambridge. In de zorg spelen gezondheidsdata en robots een steeds grotere rol.

En de wet van Moore¹⁰ blijft onverminderd van toepassing, waardoor computers steeds sneller en kleiner worden. Komende jaren zullen daarom steeds meer apparaten aangesloten worden op het internet (Internet of Things) om ons nieuwe diensten en inzichten te geven. Zoals de koelkast die ons vertelt of we nog melk hebben of de slimme weegschaal die ons vertelt hoe fit we zijn. Ook kunnen we dankzij 3D printen ongekend complexe dingen produceren en bijvoorbeeld heupimplantaten of gehoorapparaten relatief goedkoop op maat maken. Ondernemers kunnen zo -zonder enorme investeringen- producten maken. Deze technologische opmars zal de komende decennia verder doorzetten door ontwikkelingen als cloudcomputing, big data, gentech en tal van nog niet bekende uitvindingen.

9 <http://www.ad.nl/ad/nl/5597/Economie/article/detail/3338422/2012/10/27/Werknemer-bijna-4-uur-per-dag-achter-computer.dhtml>

10 De Wet van Moore is eigenlijk een voorspelling, die stelt dat het aantal transistors in een geïntegreerde schakeling door de technologische vooruitgang elke 2 jaar verdubbelt.

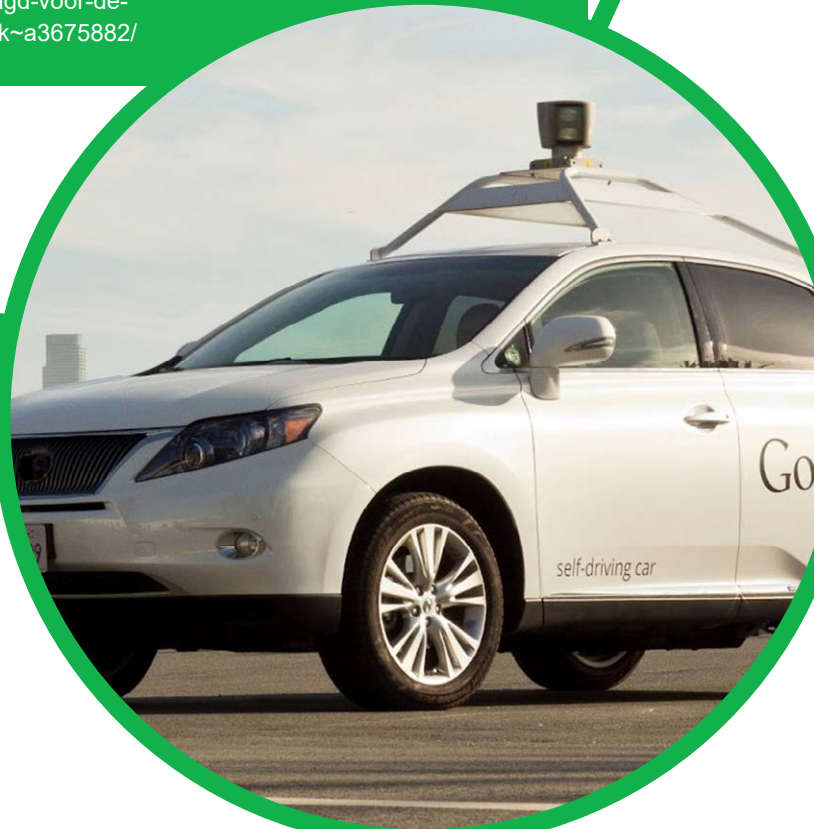
Box1: technologische ontwikkelingen

Van drones of driverless cars heeft iedereen wel eens gehoord maar veel technologie is minder bekend. Met cybernetics experimenteren we met hybride systemen van mens en machine en we verbeteren de interactie tussen beide zodat computers menselijke spraak kunnen begrijpen.

'Intelligent agents' kunnen op het web 3.0 informatie opzoeken en handelen naar hetgeen ze gevonden hebben. Machines raken in staat om op basis van grote hoeveelheden gegevens conclusies te trekken en te leren. Verschillende overheden werken momenteel aan een quantumcomputer die vele malen sneller zal zijn dan de huidige generatie (super)computers. Ook kunstmatige intelligentie reikt steeds verder. Het chatprogramma Eugene Goostman slaagde zelfs voor de Turingtest.¹¹

We zijn in staat biologisch materiaal te printen en gebruiken nanotechnologie steeds meer. We ontwikkelen nieuwe manieren om met computers te communiceren door middel van hologrammen en gesture technology en natural user interfaces.

¹¹ <http://www.volkskrant.nl/opinie/-geslaagd-voor-de-turing-test-maar-wat-betekent-dat-eigenlijk~a3675882/>



Het politieke debat ontbeert samenhang

Deze dynamiek levert maatschappelijke vraagstukken op over de impact van robotisering, digitale platforms, online profilering en cybersecurity. Maar het politieke debat gaat vooral over incidenten, zoals te dure ICT-projecten, de gehackte OV-chipkaart of cookies. Het ontbreekt aan een samenhangende visie op de invloed van technologie en internet op de samenleving van vandaag en morgen. Daarbij speelt ICT een rol in alle domeinen en sectoren terwijl bewindspersonen en Tweede Kamerleden zich vaak beperken tot hun eigen ministerie of portefeuille. Met als gevolg versnippering van de discussie en een overheid die meer dan nodig achter de feiten aanloopt.

In deze technologie visie staat D66 daarom stil bij de belangrijkste ontwikkelingen en dilemma's op het gebied van ICT en de kansen en risico's van nieuwe technologie. We hebben gesproken met meer dan 50 experts van binnen en buiten D66. In deze visie staat niet de technologie zelf centraal maar de gevolgen ervan op vier centrale gebieden van onze maatschappij, namelijk **economie, vrijheid, veiligheid en het publieke domein**. Binnen deze vier elementen komen onderwerpen als economische kansen, privacy, cybersecurity en het gebruik van ICT in onderwijs en zorg aan de orde. Zo formuleren we een sociaal-liberale visie op een passende rol van de overheid in de steeds verder digitaliserende wereld.





Visie: De overheid in een digitaal tijdperk

Technologie en maatschappelijke dilemma's

Nieuwe technologie heeft tot doel het leven gemakkelijker, veiliger en vrijer te maken. Dankzij snellere computers en betere internetaansluitingen kunnen we eenvoudig nieuwe contacten leggen of nieuwe interesses en vaardigheden ontdekken. Door het internet hebben we meer informatie dan ooit tot onze beschikking, bijvoorbeeld de enorme hoeveelheid instructievideo's op Youtube. Voor ondernemers biedt het internet de mogelijkheid om wereldwijd markten aan te boren.

Maar technologische vooruitgang kent ook risico's. Zoals het opslaan en analyseren van steeds meer persoonlijke gegevens waardoor bedrijven en overheden vrijwel alles over ons weten. Hun verzameldrift schendt onze privacy en ons opgebouwde 'profiel' bepaalt welke informatie we op ons scherm zien afgebeeld, hetgeen tot discriminatie kan leiden.¹² Omdat we steeds meer online zijn en doen wordt het voor cybercriminelen bovendien steeds makkelijker om creditcardfraude te plegen of bedrijfsgeheimen te stelen.

Digitalisering heeft ook een grote impact op onze economie, bijvoorbeeld door de snelle vorming van zeer dominante spelers in digitale markten, zoals eerst Microsoft, en nu Google en Facebook. Daarnaast hebben internettoepassingen de afgelopen decennia talloze markten verstoord en veranderd. Eerst veranderden websites de reisbranche en e-mails de postmarkt. Vervolgens veranderden Napster¹³, Kazaa en iTunes de muziek- en filmindustrie. En nu zetten Uber en Airbnb de taxi- en hotelmarkt op zijn kop.

¹² Bedrijven gebruiken alle informatie die ze over ons weten om een profiel van ons te maken, bijvoorbeeld 'sportief', 'D66-stemmer' en 'ondernemer', en op basis van die profielen zien we bepaalde advertenties of wordt soms zelfs de informatie die we zien (bijvoorbeeld het nieuws) aangepast.

¹³ De MP3 is ooit met overheidsgegeld uitgevonden door een doctorale student in Duitsland en slimme ondernemers als Shawn Fanning en Steve Jobs hebben daar dankbaar gebruik van gemaakt.

Box2: Hoe is het internet ontstaan en hoe werkt het?

De fundamenteën voor het internet zijn gelegd in wetenschappelijke artikelen in het begin van de jaren 60, vrijwel gelijktijdig geschreven aan onderzoeksinstituten MIT, RAND en NPL. Deze ideeën zijn vervolgens opgepikt door de onderzoekstak van het Amerikaanse ministerie van defensie, DARPA. Hier hebben onderzoekers de eerste vorm van internet, ARPANET, opgezet.

Cruciaal was de uitvinding van 'packet switching'. Hiermee worden gegevens opgeknipt in kleine pakketjes van data en via de kabel (of een ander medium) verstuurd. Dit lost twee problemen op. Allereerst kunnen meerdere computers tegelijk van een netwerk gebruik maken, omdat de pakketjes van verschillende computers achter elkaar door dezelfde kabel verstuurd kunnen worden. Daarvoor had je per gegevensuitwisseling, zoals een telefoongesprek, een aparte kabel nodig. Daarnaast vergroot packet switching de betrouwbaarheid van de communicatie omdat pakketjes in verschillende volgorde via verschillende kabels verstuurd kunnen worden.

Een ander punt is: hoe zorg je dat de pakketjes op de juiste plek aankomen? Daarvoor is het IP-protocol uitgevonden. Elk apparaat dat is aangesloten op het internet heeft een eigen IP-adres. Dit kan je vergelijken met een telefoonnummer. Dit zorgt, samen met het Transmission Control Protocol (TCP/IP), voor de correcte verzending en aankomst van pakketjes data tussen verschillende computers op het internet. Zo is het Internet in feite een grote, wereldwijde afspraak tussen miljoenen partijen die communiceren op basis van een lijst van standaarden die bijgehouden wordt door de IETF: de Internet Engineering Taskforce. Weinig bekend is dat het juist Nederlanders zijn die een essentiële rol hebben gespeeld in de IETF en het wereldwijd promoten van de standaarden.

In het begin bestond 'het internet' uit een klein aantal computers op verschillende universiteitscampussen. Inmiddels zijn er miljarden apparaten aangesloten. Toch blijft het internet in essentie een aantal computers die met elkaar verbonden zijn via kabels.

Bovenop deze laag van transport protocollen is een laag van applicatieprotocollen gebouwd, zoals het HyperText Transfer Protocol (HTTP) dat ook wel als de basis van het huidige wereldwijde web (WWW) gezien wordt. De internetbrowser staat bij dit protocol centraal. Als je 213.171.135.95 intypt in je internet browser dan stuurt jouw computer een HTTP-request naar de computer met dat IP-adres. Die computer (of server) stuurt vervolgens bestanden terug die samen een website vormen. Omdat het lastig is voor mensen om al die IP-adressen te onthouden is het Domain Name System (DNS) gecreëerd. Zo hoef je niet 213.171.135.95 in te typen, maar www.D66.nl.

Mens en overheid vanuit sociaal-liberaal perspectief

Het vertrouwen van sociaal-liberalen op de eigen kracht van mensen is gebaseerd op de overtuiging dat mensen ruimte en kansen moeten krijgen om zichzelf te ontplooien én dat zij daartoe – in meer of in mindere mate – moeten worden uitgedaagd, aangespoord of geholpen. Beter dan de overheid zijn zij in staat voor zichzelf en anderen een samenleving te creëren die open, dynamisch en duurzaam is. De vrijheid die deze ontplooiing mogelijk maakt, moet steeds worden bevocht. De grens, waar de vrijheid van de een die van de ander schaadt, staat niet vast, maar is het resultaat van wat redelijke mensen samen van tijd tot tijd als begrenzing vaststellen. De moderne staat is ooit opgericht om de vrijheid van individuen te vergroten door een aantal fundamentele vrijheden te beschermen, zoals de vrijheid van meningsuiting, vrijheid van godsdienst of de vrijheid om jezelf te ontwikkelen, om te zijn wie je bent en je dromen na te jagen.

Verschillende rollen voor de overheid in het digitale domein

In de fysieke wereld vinden mensen het vanzelfsprekend dat de overheid verantwoordelijk is voor (de toegang tot) bepaalde behoeften, zoals zorg, onderwijs en infrastructuur, en tevens normen stelt, regels maakt en besluiten neemt over tal van zaken die de levens van mensen raken: ruimtelijke inrichting, economische activiteiten en de rechtstaat.

Ook in de digitale wereld heeft de overheid deze belangrijke taak. Tegelijk liggen de grenzen in het digitale domein ingewikkelder. Technologische ontwikkelingen op het gebied van ICT en internet bieden zoveel nieuwe mogelijkheden dat het nodig is om de grens, waar de vrijheid van de een die van de ander schaadt, te herijken, evenals de verantwoordelijkheid van de overheid om de macht van anderen (individueel, bedrijven of overheden) te begrenzen en om ervoor te zorgen dat mensen de kansen van digitalisering kunnen grijpen en de bedreigingen het hoofd kunnen bieden.

De overheid acteert hierbij vanuit verschillende rollen. Zo is de overheid hoeder van vrijheid, beschermt zij ons tegen criminelen, is scheidsrechter richting mensen en bedrijven, financier van innovatie en initiatieven en inkoper van zowel ICT hard- als software. De overheid kan individuen ook op economisch gebied meer vrijheid geven door ruimte te bieden om nieuwe, innovatieve producten of diensten te ontplooien.

De visie van D66: Nederland in 2030

Vanuit deze sociaal-liberale blik op de samenleving kijkt D66 naar technologie en toekomst. Het verleden heeft bewezen dat grote technologische ontwikkelingen zoals automatisering van de landbouw, industrialisatie en nu digitalisering en automatisering



de kwaliteit van leven vergroten.¹⁴ In plaats van vooruitgang proberen tegen te houden is het beter om voorop te lopen door ons aanpassingsvermogen te vergroten en zo snel mogelijk mee te bewegen. Met oog voor de nadelen en de verliezers van verandering. Wat D66 betreft is Nederland in 2030 digitale koploper in Europa: een broedplaats, een thuishaven en een trekpleister voor innovatieve bedrijven en talentvolle individuen, die voor een nieuwe digitale gouden eeuw zorgen. Nederland is in 2030 een aantrekkelijke vestigingsplaats dankzij de beste digitale infrastructuur en is daarnaast een proeftuin voor digitale producten en diensten, zoals robots, drones, zelfrijdende auto's en IoT-apparaten. De Nederlandse overheid handhaaft een eerlijk speelveld voor gevestigde bedrijven en hun uitdagers en dringt daar ook in Europa op aan.

Ook is Nederland een veilige haven voor persoonsgegevens. Nederlanders kunnen bewuste keuzes maken om hun privacy te beschermen tegen grote data verzamelende bedrijven en overheden beperken de gerichte opslag en het gebruik van data tot wat echt noodzakelijk is. Bovendien is Nederland een toevluchtsoord voor ethische hackers en onderzoekers die beschermd en beloond worden als ze bedrijven en overheden helpen fouten te vinden in producten of ICT-systemen.

Nederlanders hebben de juiste vaardigheden om gebruik te maken van de ontwikkeling van digitalisering. Ook hebben zij grip op de digitale kansen en de risico's op het gebied van economie, cybersecurity en privacy. De toegenomen hoeveelheid data wordt op een overzichtelijke en veilige wijze ontsloten om mensen meer keuzevrijheid en regie over bijvoorbeeld hun zorg en onderwijs te geven.

Om deze stip op de horizon te bereiken zijn vergaande stappen nodig op het gebied van economie, vrijheid, veiligheid en het publieke domein. Deze stappen worden in de volgende hoofdstukken nader toegelicht.

¹⁴ Een boek dat de voortdurende vooruitgang door specialisatie, innovatie en handel op basis van overtuigende feiten en cijfers schetst, is "De rationale optimist" van Matt Ridley (2010).

Box3: Uitgangspunten voor D66

Economie:

- Omarm vooruitgang met oog voor de nadelen
- Aanpassingsvermogen is een cruciale factor
- Maak technologie-neutrale regels en handhaaf deze

Vrijheid:

- Garandeer een vrij en open internet
- Je persoonsgegevens blijven van jou
- Data en profielen mogen niet discrimineren

Veiligheid:

- Vrijheid en veiligheid gaan prima samen
- Wat offline niet mag, mag online ook niet
- Massale dataopslag maakt ons onveilig

Publieke Domein:

- Stel de mens en niet de techniek centraal
- Niet alles wat kan, is wenselijk
- Digitaal mag niet asociaal betekenen



Hoofdstuk 1

De Interneteconomie

In 1866 kon de eerste trans-Atlantische telegraafkabel 34 tekens per minuut versturen. In 1920 kostte het versturen van een telegram ongeveer 5 euro. Een tweet is nu gratis en gaat binnen een seconde de hele wereld over. Toen NASA in 1969 twee astronauten op de maan zette had het minder computerkracht dan een gemiddelde smartphone nu. De Cray 2 supercomputer uit 1985, met een prijskaartje van zo'n €14 miljoen, is ruim 15 keer langzamer dan een Iphone 5 van €400 euro. Twintig jaar geleden begon internetten met een minuut lang hels lawaai van de inbelmodem.

De uitvinding van computer en internet zijn de basis van de derde industriële revolutie. ICT is van grote invloed op de economische groei en het werk dat we doen. De ICT-sector groeit jaarlijks bijna drie keer zo snel als de rest van de Nederlandse economie en wordt steeds belangrijker. In 2014 waren 336.000 ICT'ers werkzaam. Vrijwel elk bedrijf gebruikt ICT in zijn bedrijfsprocessen. Deze ontwikkelingen veranderen de fysieke wereld: winkels verdwijnen langzaam maar zeker uit onze binnensteden en ieder huis is een potentieel hotel. Bedrijfskosten dalen: een website hoeft niet meer te kosten dan tien euro per maand en met een enkele upload in een online winkel voor apps, software, muziek of boeken is je product beschikbaar voor gebruikers over de hele wereld, met marginale meerkosten.¹⁵

Deze ontwikkelingen voltrekken zich wereldwijd. De meeste nieuwe internetgebruikers komen inmiddels uit Afrika en Azië. Het aantal Ghanezen met een mobiele telefoon is bijvoorbeeld gestegen van 10% in 2002 naar 89% in 2015, een cijfer dat vergelijkbaar is met de situatie in Europa. Steeds vaker zien we dat ontwikkelingslanden trendsetters worden. Over mobiele betalingen kan Europa bijvoorbeeld nog veel leren van Afrika. Digitalisering is een belangrijk wapen tegen corruptie door de economie te formaliseren en de 'middleman' uit te sluiten. In Afghanistan ontvangen politiemannen 30% meer salaris sinds deze mobiel wordt ontvangen. En in Mexico en Brazilië krijgt de overheid zicht op de economie door elektronische facturatie. Niet voor niets zeggen de Belgische vicepremier Alexander de Croo of de Zweedse oud-premier Carl Bildt dat internet bovenaan de ontwikkelingsagenda zou moeten staan.¹⁶

Disruptieve doorbraken bonken op de deur. Robotisering, Smart Factories, Big Data, Internet-of-Things, cloudtechnologie, quantumcomputers, kunstmatige intelligentie,

¹⁵ Jeremy Rifkins – The Zero Marginal Cost Society.

¹⁶ <http://www.volkskrant.nl/opinie/zet-internet-boven-aan-ontwikkelingsagenda~a4134376/>

DNA-genomen, zelfrijdende auto's, het aantal voorbeelden is eindeloos. Al deze ontwikkelingen bieden nieuwe kansen maar zijn ook potentieel ontwrichtend. Dit geeft de overheid een verantwoordelijkheid.

Nederland is goed gepositioneerd om van deze nieuwe wereld te profiteren.¹⁷ De penetratiegraad van internet, snelle netwerken, smartphones en innovatieadoptie is hier erg hoog. Daarnaast hebben we veel datacenters, app-bouwers, toonaangevende digitale ondernemingen als SURFNET, ASML, FOX-IT en de vele innovatieve startups rondom brainports als Eindhoven, Groningen, Amsterdam en Twente. Onze thuismarkt en schaalbaarheid¹⁸ zijn beperkt maar er is de mogelijkheid om Nederland te positioneren als proeftuin voor innovatie en als West Coast van Europa. Alle belangrijke innovatieve regio's zijn in internationaal perspectief binnen steenworpafstand. Desondanks raken we internationaal achterop.¹⁹ Ons onderwijs sluit onvoldoende aan op de digitale wereld en jonge, innovatieve bedrijven lopen tegen onnodige barrières aan. Er valt voor Nederland nog een hele digitale wereld te winnen.

Visie 2030: Nederland als digitale koploper van Europa

Nederland is in 2030 met zijn compacte schaal, hoogwaardige infrastructuur en hoogopgeleide bevolking de trekpleister, broedplaats en thuishaven van de Europese interneteconomie. Naast de Rotterdamse haven en Schiphol is een derde, digitale mainport ontstaan waarmee we ook de digitale toegangspoort van Europa zijn geworden.

Nederland kent een bloeiende industrie van jonge innovatieve bedrijven die de gevestigde orde uitdagen. Talent kiest er steeds vaker voor een eigen onderneming te starten. Met één digitale Europese markt is een groot aantal problemen die Nederlandse startups voorheen hadden op het gebied van schaalbaarheid en het vinden van financiering opgelost.

Nederland staat internationaal bekend om zijn goede vestigingsklimaat en eigentijdse regelgeving en bestemming waar belangrijke randvoorwaarden als privacy en de

17 Nederland bezet de zesde plaats op zowel de ranglijst van landen met snel internet volgens Akamai Technology's State of the Internet (de meest geavanceerde ICT-ontwikkeling van VN-organisatie ITU) als op de ranglijst van InternetLiveStats over het % inwoners met toegang tot het internet. Daarnaast zijn we hoogopgeleid, we staan vierde op de 'education index' van UNDP en zijn internationaal georiënteerd.

18 Eén van de grote voordelen van de nieuwe interneteconomie is dat elke onderneming in principe direct een wereldwijd bereik heeft, maar in werkelijkheid zorgen nationale verschillen en regelgeving ervoor dat het betreden van elke nieuwe markt drempels kent, waardoor de omvang van de thuismarkt in de praktijk bepalender is dan in theorie noodzakelijk.

19 "Where the Digital Economy is moving the fastest" (Harvard Business Review, gebaseerd op "Digital Planet: Ready for the Rise of the e-Consumer": <http://fletcher.tufts.edu/~media/Fletcher/Microsites/Planet%20eBiz/Digital%20Planet%20-%20Executive%20Summary.pdf>)

veiligheid van data gewaarborgd zijn. Hierdoor kiezen steeds meer buitenlandse bedrijven voor Nederland als vestigingsplaats. Dit is mede te danken aan het feit dat Nederland geen symboolwetten heeft doorgevoerd die het vertrouwen in de digitale technologie schaden en databescherming ondermijnen. Ook is Nederland erin geslaagd successen nog beter uit te venten dan het geval was met AMS-IX of de enige Nederlandse ‘unicorn’²⁰ Adyen, maar ook WiFi en Bluetooth van wie de bedenkers een Nederlands paspoort hadden.

Aanbevelingen

De hierboven beschreven situatie is zeker realiseerbaar. Voorwaarde is wel dat we zorgen voor een uitmuntend digitaal vestigingsklimaat. D66 stelt daarom het volgende voor:

Maak radicaal ruimte voor vernieuwing...

Nederland (Europa!) benut de kansen van ICT en internet onvoldoende. Alle top 10 internetbedrijven zijn Amerikaans of Chinees. Het eerste Europese bedrijf, ASOS.com staat op nummer 19. Digitale innovatie komt van nieuwe, disruptieve spelers. Echter, bestaande regelgeving is vaak niet goed uitgerust op de diensten die zij aanbieden. Uber brak een markt open die gedomineerd werd door hoge prijzen en slechte service. Het bedrijf was dus succesvoller dan de door de overheid bedachte taxicertificaten. Toch wordt Uber afgerekend op het ontbreken van deze certificaten.

We moeten achterhoedegevechten staken en anticiperen op onvermijdelijke veranderingen, ook in onze wetgeving. Vooral kleine en startende ondernemingen hebben last van verouderde regels, omdat zij geen geld hebben voor aanpassingen of rechtszaken. In plaats van het verdedigen van gevestigde belangen op basis van regels uit het vorige millennium moet de overheid zorgen voor eerlijke concurrentie tussen alle spelers in een markt. Daartoe moet het doel –niet het gekozen nalevingsmiddel- van een wet centraal komen te staan. Dit kan door regels technologie-neutraal te maken. Bijvoorbeeld door taxi’s niet langer verplichten een factuur in de auto uit te printen maar deze binnen een bepaalde tijd te verstrekken, zodat (milieuvriendelijkere) alternatieven als het mailen van een PFD-factuur mogelijk worden.

Op verzoek van D66 is minister Kamp (EZ) in 2014 begonnen met de modernisering van onder meer de taxiwet, de drank- en horecawet, de rijtijdenwet maar bijvoorbeeld ook regels over vergoeding van 3D geprinte implantaten. D66 ziet hierin een goede eerste stap maar pleit voor een kabinetsbrede operatie om wetten en regels klaar te maken voor het digitale tijdperk.²¹ Naast wetgevingsruimte pleit D66 ook voor voldoende fysieke plekken waar innovatie plaats kan vinden, zoals goede testlocaties voor drones of zelfrijdende auto’s en kleine proeftuinen waar ondernemers prototypes kunnen testen (FabLabs).

20 Een startup met een waarde van meer dan een miljard euro.

21 Een vergelijkbare aanpak als bij ‘Keuzes in Kaart’ waarbij elk ministerie zijn aandeel moest leveren.

Box4: Digitale spraakverwarring versus technologie neutrale wetgeving

Veel termen in bestaande wetgeving gaan gedeeltelijk voorbij aan de weerbarstige praktijk van digitalisering. Zo zijn over de betekenis van de wettelijke term ‘persoonsgegevens’ vele pagina’s volgeschreven en krijgt het (Europeesrechtelijke) begrip nog steeds nadere invulling via jurisprudentie.²²

Ook in nieuwe wetgeving doet zich spraakverwarring voor. De wet computercriminaliteit III voorziet bijvoorbeeld in de mogelijkheid tot het binnendringen in “geautomatiseerd werk” met het oog op opsporing. Geautomatiseerd werk omvat alle informatietechnologie, in de meest ruime zin van het woord, inclusief auto’s, thermostaten en koelkasten. In een smartphone binnendringen is echter heel anders dan in een computer, dus dient de vraag zich aan of er wellicht een onderscheid gemaakt moet worden tussen type activiteiten.

Hoe lastig deze spraakverwarring ook is, te specifieke en technologieafhankelijke formulering is niet de oplossing want het maakt wetgeving juist contraproductief, zoals we gezien hebben bij de cookiewetgeving. Daarom moet zoveel mogelijk gekozen worden voor technologieonafhankelijke formuleringen en moeten de reikwijdte van wetten primair gezocht worden in afbakeningen (van definities) die los staan van een specifiek apparaat of een specifieke technologie.

...En help verliezers van vooruitgang mee vooruit (vrees robots niet!)

Veel nieuwe technologieën laten bestaande banen verdwijnen. Van zelfrijdende auto’s tot robots die artsen vervangen bij operaties. Volgens Amerikaans onderzoek zal de komende twintig jaar de helft van de huidige banen in de VS hierdoor verdwijnen.²³ In Nederland ligt dat op ongeveer 40%.²⁴ Dat klinkt heftig maar is niets nieuws. Tijdens de Industriële Revolutie maakte de automatische weefmachine in Engeland een sector van 250.000 wevers overbodig.²⁵ De gevolgen waren voor deze groep natuurlijk enorm, maar uiteindelijk gingen de leefomstandigheden

22 <https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wbp-naslag/hoofdstuk-1-algemene-bepalingen-art-1-tm-5/artikel-1-sub-wbp>

23 http://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf

24 Rathenau over Robotisering: Deloitte 2014.

25 De Luddieten. Zij legden de basis voor de term luddisme: een sociale beweging in het Engeland van begin 19^e eeuw die zich verzette tegen industriële en technologische vooruitgang.

meer omhoog dan de werkeloosheid. Het historische patroon is steeds geweest dat technologische vooruitgang banen vernietigt in oude sectoren en banen schept in nieuwe sectoren.

Maar met de computer ging een machine na spierkracht ook denkwerk van mensen overnemen. Mensen kunnen zich weliswaar nog steeds onderscheiden, bijvoorbeeld via creatief of empathisch werk, maar dat neemt niet weg dat bepaalde beroepstypen of -sectoren overbodig worden. Ook moeten we voorbereid zijn op tijdelijke of regionale werkeloosheid. De automatiseringsgolf treft nu vooral de middenklasse. De hoogopgeleide, internationaal concurrerende talenten zien hun marktwaarde (nog?) stijgen, terwijl laagopgeleide banen (voorlopig?) overblijven in de dienstverlening van kappers, tuiniers en klusjesmannen die zich moeilijk laten automatiseren.

De grote ongelijkheid die kan ontstaan uit het uithollen van de middenklasse is volgens Stephen Hawking een van de grootste bedreigingen voor de toekomst.²⁶ Economieprofessor Richard B. Freeman (Harvard University) schrijft dat toenemende ongelijkheid en robotisering samen dreigen te zorgen voor modern feodalisme waarin kapitaalbezitters de macht over economie en maatschappij hebben. Niet het gebrek aan werk maar de oneerlijke voordelen van de machine-eigenaren vormen dan het grootste probleem. En in een *Open brief over de digitale economie*²⁷ schrijft een grote groep wetenschappers dat de voordelen van technologische vooruitgang ongelijk verdeeld zijn.

Terechte zorgen. Maar tegelijk is technologische vernieuwing niet te stoppen en helpt robotangst niemand aan het werk. Bovendien geeft robotisering volgens studies van zowel het Rathenau Instituut als de Wetenschappelijke Raad voor het Regeringsbeleid (WRR)²⁸ uitzicht op meer groei en hogere arbeidsproductiviteit. Daarbij worden de snelheid en de omvang van de gevolgen van digitalisering vaak overdreven: menselijke arbeid wordt meestal niet volledig vervangen door robots maar aangevuld. En de mens blijft de baas en ook degene die beslissingen neemt. In plaats van vrezen wat de computer allemaal kan gaan doen moet de mens bepalen wat hij zelf wil blijven doen.²⁹

D66 wil dat de overheid digitalisering en robotica omarmt en erin investeert, belemmeringen wegneemt, de organisatorische versnippering doorbreekt en zorgt voor betere samenwerking of – zoals de WRR het noemt – ‘co-creatie’ tussen alle betrokkenen, leidend tot mensgerichte automatisering (Carr, 2015). D66 deelt

26 <http://money.cnn.com/2015/10/12/news/economy/stephen-hawking-technology-inequality/index.html>

27 <http://openletteronthedigitaleconomy.org>

28 Respectievelijk: “Werken aan de Robotsamenleving” (Rathenau Instituut, 2015) en “De Robot de baas” (WRR, 2015). Van beide rapporten is in deze paragraaf dankbaar gebruik gemaakt.

29 In dit opzicht wordt vaak verwezen naar automatische piloten. Weinig mensen zouden in een vliegtuig stappen waar geen menselijke piloot aanwezig is. Zelf zeggen veel menselijke piloten dat elke vlucht zou mislukken als je alle regels gehoorzaam zou volgen. Improvisatie is blijkbaar nodig.

de analyse dat een menselijke 'robotsamenleving' (Rathenau Instituut) of een 'inclusieve robotagenda' (WRR) meer vraagt dan meer onderwijs, sociaal beleid en moderne regelgeving.

Omdat onderwijs het niet meer vanzelfsprekend wint van technologie en omdat ook steeds meer hogeropgeleide taken door robots worden overgenomen, is een diploma alleen niet genoeg. Naast het levenslang leren moet de focus in het onderwijs verlegd worden om zijn meerwaarde te behouden: meer gericht op de 'complementariteit' (WRR) tussen mens en machine en meer gericht op vaardigheden waarin mensen zich onderscheiden van computers (probleemoplossend vermogen, creatieve en sociale vaardigheden).

De overheid moet (mogelijke) verliezers van technologische ontwikkeling helpen. Sociale vangnetten blijven daarbij uiteindelijk nodig maar het verbeteren van de positie van werknemers, het behoud van arbeidsplezier en het beschermen van arbeidskwaliteit (de WRR wijst hierbij op 'eigenaarschap') is minstens zo belangrijk. Met als doel om de voordelen van digitalisering zo goed mogelijk te verdelen. Om het –met automatisering verbonden- verdelingsvraagstuk tegemoet te treden en onwenselijke concentratie van macht en vermogen te voorkomen, is een actieve overheid nodig. Door wetenschappers gedane suggesties als een 'robotdividend',³⁰ werknemers-aandeelhouderschap (Freeman, 2015) of 'public venture funds' (Rodrik, 2015) zijn daarbij nuttiger dan het idee van een basisinkomen (dat grotendeels voorbij gaat aan het verdeelvraagstuk en aan het idee van werk als een vorm van zelfontplooiing).

Tot slot zal een deel van de mensen die hun baan verliezen hun diensten aanbieden via platforms. Zoals tijdens de Industriële Revolutie, toen de stoommachine veel geschoolde arbeiders werkeloos maakte en naar fabrieken dreef. Het grote aanbod van werknemers en het gebrek aan regels over de nieuwe technologie veroorzaakten slechte werkomstandigheden en lage lonen, totdat de overheid hier een einde aan maakte. Ook de chauffeurs van Uber en klusjesmannen bij Helply zijn overgeleverd aan de tucht van het platform voor zaken als veilige werkomstandigheden, het gemaakt aantal werkuren en privacy. Het is daarom nodig goede sociale regels te maken voor deze fabrieken van de 21^e eeuw en de positie van de ZZP'ers te verstevigen.³¹

30 Brynjolfsson en McAfee (2015)

31 Onder meer door meer individuele keuzevrijheid over pensioen en arbeidsongeschiktheidsverzekering.

Box5: Lessen uit eerdere Industriële Revoluties

Angst voor werkeloosheid door technologische vooruitgang is zo oud als de weg naar Rome. Aristoteles besprak in zijn *Politika* al de mogelijkheid dat machines menselijke arbeid zouden laten verdwijnen. Innovatie is dan ook vaak met argusogen bekeken. In de Middeleeuwen werkten Gilden innovatie actief tegen, koningin Elizabeth I weigerde een patent te verlenen aan een nieuwe breimachine uit vrees voor de textielsector en de Luddieten kwamen in gewelddadige opstand tegen de machines ten tijde van de Industriële Revolutie. Ook denkers als David Ricardo, John Stuart Mill, Karl Marx en Gandhi vreesden baanvernietiging door technologische ontwikkeling.

Deze ideeën staken de kop op bij hoge werkeloosheid om te verstommen wanneer de banengroei aantrok. Steeds weer compenseerden economische groei en structureel betere levensstandaarden de tijdelijke nadelen. De automatische weefmachine maakte een einde aan een sector waarin 250.000 Engelse werknemers de kost verdienden, maar zorgde dat nieuwe kleding niet meer was voorbehouden aan een select groepje rijken. Technologische ontwikkeling zorgt zo voor goedkopere producten, meer consumptie en als gevolg daarvan meer banen. De kolenarbeider maakte plaats voor de telegrambezorger die op zijn beurt plaats maakte voor de webdesigner.

Angst voor banenvernietiging komt vaak uit het idee van een vaste hoeveelheid werk, de ‘lump labour fallacy’. Dit gaat voorbij aan het feit dat mensen hun toegenomen welvaart graag inzetten in het bevredigen van nieuwe behoeften. Nadat iedereen zich in nieuwe kleren had kunnen steken, richtte men zich op de wekelijkse scheerbeurt. Zo zal er steeds vraag naar nieuwe arbeid blijven en zullen nieuwe sectoren ontstaan.³² Hoe en wat kan niemand voorspellen en logisch lijkt het ook niet altijd: zo gaat digitale technologie gepaard met de renaissance van de lokale maakindustrie.

De overheid moet dergelijke transities goed begeleiden. Door werkomstandigheden te bewaken en door voorwaarden te scheppen bij nieuwe ontwikkelingen. Zo speelden overheden een rol in de aanleg van een spoorwegennetwerk dat de weg baande naar een industriële samenleving.

Fors meer investeren in onderzoek en innovatie

De overheid is een belangrijke aanjager van innovatie. Microprocessors, harde schijven, LCD-schermen, lithium-ion-batterijen, http, html, het internet, gps, SIRI, klikwielnavigatie, multi-touch-screens zijn stuk voor stuk gevolg van overheid-gefinancierd onderzoek. Onderzoek loont dus. Daar komt bij dat overheden vaak investeren in projecten die in de private markt geen bestaansrecht hebben. Venture Capital fondsen (VC's) verwachten binnen drie tot vijf jaar opbrengst uit hun investering, uiterlijk tien. De investeringscyclus van overheden is vijftien à twintig jaar. Nederland dankt de aanwezigheid van superknooppunt AMS-X (sinds 1997) aan goede samenwerking tussen publieke en private partijen. Het later hieraan gekoppelde Gigaport-project werd zelfs gefinancierd met overheidsgeld. Een duidelijke ambitie op het gebied van Big Data of 3D printen zou opnieuw een katalysator kunnen betekenen.

Nederland heeft zich tot doel gesteld in 2020 2,5% van het BBP uit te geven aan onderzoek en innovatie. Van die 2,5% moet 1% publiek geld zijn. Volgens het Rathenau Instituut gaan we die doelstelling niet halen.³³ Sterker nog, dit kabinet geeft er steeds minder aan uit. D66 wil die neergang stoppen en minimaal €1 miljard meer investeren in onderzoek en innovatie. Ook Europa moet meer investeren in innovatie. D66 wil de helft van die landbouwsubsidies gaan investeren in onderzoek, onderwijs en innovatie.

Maak investeren in startups aantrekkelijker

Amerikaanse startups halen makkelijker geld op dan Europese. Bovendien groeien ze sneller door en vinden eenvoudiger een exit. De Amerikaanse Venture Capital sector is groter, investeringsrondes zijn groter en bedrijven als Google, Facebook en Amazon kopen bijna wekelijks startups.

D66 is voorstander van een Europese kapitaalmarkt. Want hoewel de Europese economie vergelijkbaar is met de Amerikaanse, is de Amerikaanse kapitaalmarkt ongeveer vijf keer zo groot. Om te voorkomen dat startups worden weggekocht zodra ze succesvol zijn, moeten we dit gat dichten. Ook in Nederland kunnen we stappen zetten. Om te beginnen moeten we *SEED investeringen*³⁴ fiscaal stimuleren. Het Verenigd Koninkrijk doet dit via de succesvolle SEIS regeling (Small Enterprise Investment Scheme) waarmee een investeerder een deel van zijn investering kan aftrekken van de vermogenswinstbelasting.

33 <https://www.rathenau.nl/nl/publicatie/total-investment-research-and-innovation-twin-2013-2019>

34 SEED investeringen zijn relatief kleine investeringen van €10.000 tot €100.000 die bedoeld zijn om een bedrijf op te kunnen starten en een eerste versie van een product of dienst te kunnen maken.

Ook moeten Nederlandse institutionele beleggers meer in Nederlandse Venture Capital (VC) fondsen beleggen, zodat meer geïnvesteerd kan worden in startups. Het Dutch Venture Initiative (DVI) moet daarvoor zorgen. Nu beleggen institutionele beleggers vooral in Amerikaanse VC fondsen die vervolgens in Nederlandse startups investeren en hen naar de VS halen. D66 wil het DVI daarom aantrekkelijker maken zodat pensioenfondsen meer in Nederlandse startups investeren.

D66 wil verder dat de overheid meer SBIR-programma's uitschrijft.³⁵ Zo komt er op initiatief van D66 een SBIR-programma om mensen met een verstandelijke beperking te helpen, bijvoorbeeld door middel van speciale agenda of openbaar vervoer apps. Tot slot is het cruciaal dat een startup het opgehaalde geld kan inzetten om te groeien. Daarom pleiten we al langer voor een Startup BV.

Box6: Startup BV 2.0

Al in de jaren '50 stimuleerde de Amerikaanse overheid de opkomst van Venture Capital fondsen met het succesvolle Small Business Investment Company (SBIC) programma. Bedrijven als Apple, AOL, Intel en HP komen hieruit voort. In 1982 begon het Small Business Innovation Research Programma waar bedrijven als Symantec, Qualcomm en iRobot (bekend van de Roomba stofzuigers) uit voort kwamen.

Bedrijven als Google, Facebook en Apple kopen jaarlijks tientallen startups. De oprichters van die startups beginnen vervolgens weer nieuwe bedrijven of investeren in andere startups. Zo ontstaat een dynamisch startup-ecosysteem. Neem Paypal, in 2002 gekocht door Ebay. De oprichters, en enkele medewerkers, hebben na de verkoop meerdere miljardenbedrijven opgericht, zoals Tesla, LinkedIn, Youtube, Yelp en SpaceX. Nederland heeft niet zo'n cultuur van overnames.

Daarom heeft D66 met startup-oprichters, investeerders en andere belanghebbenden gesproken. Met als conclusie dat startups makkelijker kunnen doorgroeien door hen enkele uitzonderingen³⁶ te geven. Dit kan via een aparte rechtsvorm of anders een vinkje in het KvK-register. Om misbruik te voorkomen moet een startup het vinkje samen met een S&O verklaring aanvragen bij de RVO.

35 SBIR is een afkorting voor Small Business Innovation Research. SBIR is een manier om ondernemers uit te dagen innovaties te ontwikkelen op bepaalde maatschappelijke uitdagingen. Ondernemers kunnen hun idee opsturen, waarna de ondernemers met de beste ideeën een opdracht voor een haalbaarheidsonderzoek krijgen. De ondernemers met de meest kansrijke haalbaarheidsonderzoeken krijgen opdracht hun product verder te ontwikkelen.

36 Zie: <https://d66.nl/content/uploads/sites/2/2015/02/D66-Startup-BV-v8.pdf>.

Benut de mogelijkheden van open data

De overheid moet databestanden zoveel mogelijk open aanbieden. Burgers moeten toegang hebben tot zoveel mogelijk publieke informatiebestanden die met belastinggeld zijn aangelegd. Niet alleen om de overheid ter verantwoording te kunnen roepen, maar ook om problemen op te lossen. Open data schept economische kansen als bedrijven bestaande informatie benutten voor diensten of applicaties. Zonder de open data van het KNMI hadden we geen Buienradar gehad. De Europese Commissie schat het potentieel van open data in Europa op 140 miljard euro.³⁷ Hetzelfde geldt voor de data van semi-overheidsorganisaties als de Kamer van Koophandel. Omdat bedrijven zich verplicht inschrijven in het handelsregister, wil D66 de informatie hierin vrij beschikbaar maken.

Burgers zijn vaak verplicht data met de overheid te delen. Dat betekent dat je als overheid een extra plicht hebt om de privacy van de personen in kwestie te waarborgen. Vooral wanneer door slimme interpretatie van open data persoonsgegevens te herleiden zijn. De overheid moet de burger dan ook beschermen tegen misbruik van open data. Open data zijn geen kwaad dat bestreden moet worden; degene die misbruik maken van open data zijn dat wel.

In Nederland behoren wij met het actieplan Open Overheid tot de internationale voorhoede maar het kan beter. Frankrijk en Groot Brittannië hebben bijvoorbeeld als eerste Europese landen een 'Chief Data Officer' (CDO). Deze zorgt voor betere doorstroming van gegevens binnen overheidsinstellingen en houdt oog op de open datastrategie van de overheid. Een CDO kan ervoor zorgen dat elk ministerie proactief overheidsinformatie ontsluit en dat op een goede manier doet zodat bedrijven ermee aan de slag kunnen.³⁸

Box7: Open Data, Open Source, Open Standaard

Open data zijn data die vrij gebruikt kunnen worden, hergebruikt kunnen worden en opnieuw verspreid kunnen worden door iedereen - onderworpen enkel, in het uiterste geval, aan de eis tot het toeschrijven en gelijk delen. Open Source is software waarvan de broncode openbaar is en vrijelijk verspreid mag worden, zodat iedere enthousiaste programmeur toevoegingen of verbeteringen kan aanbrengen of fouten kan opsporen. Open standaard hard- en software is publiekelijk beschikbaar. De specificaties mogen vrij van licentierechten worden toegepast, gebruikt en gehanteerd. PDF is een goed voorbeeld.

37 Petra Pronk in iBestuur: "Open data voor beter beleid en besparingen" (december 2014).

38 Nu is een bedrijf bezig de open data van de overheid zo te bewerken dat het voor andere bedrijven goed te gebruiken is: <https://overheid.io>.

Ontwikkel integraal beleid rond de derde mainport

Naast Schiphol en de haven van Rotterdam is de digitale infrastructuur de derde mainport. Vooralsnog investeert de overheid alleen in de ontwikkeling van de eerstgenoemde mainports en is er een overlegstructuur ontwikkeld bij beide mainports waarin met alle stakeholders beleid en strategie wordt ontwikkeld om de groei te optimaliseren. Een zelfde inzet is nodig om een duurzame groei van de derde mainport te stimuleren. Daar is samenwerking en afstemming nodig tussen de digitale delta, relevante infrastructuur partijen en beleidsinitiatieven als smart industry en smart cities.

Van Topsectoren naar maatschappelijke domeinen

De manier waarop we het onderzoeks- en innovatiegeld uitgeven moet gemoderniseerd worden. Een groot deel gaat nu via het topsectorenbeleid naar verouderde sectoren en gevestigde bedrijven. Een gebrek aan keuzes staat nieuwe innovaties in de weg. D66 wil het topsectorenbeleid afschaffen en het innovatiebeleid richten op maatschappelijke uitdagingen (klimaatverandering, grondstoffenschaarste en *healthy ageing*) en veelbelovende technologieën. Hierbij kunnen we een voorbeeld nemen aan het Duitse Industrie 4.0-programma.³⁹ Nederland heeft wel een *Smart Industry* beleid, maar dit komt nog onvoldoende van de grond door een gebrek aan geld en regie.⁴⁰

Ook moeten we meer geld vrijmaken voor onderzoek vanuit wetenschappelijke nieuwsgierigheid, los van de invloed van overheid en bedrijven. Zo komen we tot écht baanbrekende innovatie. Uitdaging is het laten terugvloeien van private winsten uit deze innovaties zodat deze opnieuw in onderzoek geïnvesteerd kunnen worden. D66 wil dit probleem oplossen. De opbrengsten hiervan gaan naar een innovatiefonds dat zich toelegt op financiering van onderzoek en innovatief ondernemerschap.⁴¹

Bewaak eerlijke concurrentie op het digitale speelveld

De mondiale reikwijdte van digitale diensten werkt machtsmisbruik in de hand, zoals we eerst zagen bij Microsoft met Internet Explorer⁴² en nu bij Google dat van Eurocommissaris Margrethe Vestager het verwijt van gedwongen winkelnering krijgt.⁴³ Ook platforms zijn als gevolg van netwerkeffecten gevoelig

39 De Duitse overheid investeert ongeveer €200 miljoen om onderzoek op dit gebied te stimuleren in de wetenschap, bedrijfsleven en overheid.

40 <https://d66.nl/investeer-in-de-economie-van-de-toekomst/>

41 Mazzucato suggereert in haar boek *De Ondernemende Staat* (2014), innovaties uit te brengen onder een creative commons licentie die bedrijven kunnen afkopen voor commercieel gebruik.

42 Microsoft misbruikte de macht die ze hadden op het ene terrein (de markt voor besturingssystemen) om de overhand te krijgen in een andere (de markt voor internetbrowsers).

43 Zoekmachine Google Search (95% marktaandeel in Europa) zou eigen aanbiedingen bevoordelen en Android (op 80% van de smartphones) zou softwarefabrikanten dwingen Google apps prominent weer te geven.

voor monopolies. Nadat een partij zich als marktleider heeft gevestigd, is het voor uitdagers moeilijk om marktaandeel te veroveren. Zelfs Google+ werd nooit een reëel alternatief voor Facebook. Er zijn moderne mededingingsregels nodig om te voorkomen dat een langdurige ‘winner takes it all’-situatie ontstaat. Platforms maken via hun zoekmachines, social media en appstores eigen regels in de vorm van aankoopvoorwaarden en privacy-instellingen. D66 wil niet alleen dat die begrijpelijk uitgelegd worden aan gebruikers maar ook dat internetbedrijven zich aan de Nederlandse wet houden.⁴⁴ Naast Europa als belangrijkste consumentenbeschermers in de digitale economie moet ook de Autoriteit Consument en Markt (ACM) voldoende middelen en capaciteit krijgen om eerlijke concurrentie in het digitale domein te bewaken.

Overigens is de macht van grote bedrijven tanende. Het aantal verschuivingen in de Fortune 500 was nooit groter dan in het afgelopen decennium.⁴⁵ Daarnaast bevinden digitale ‘monopolisten’ zich in zeer competitieve markten. Er is geen enkel technologiebedrijf met een absoluut monopolie: Facebook heeft in de markt voor sociale media te maken met Twitter, LinkedIn, Tumblr, Medium en Weibo. Google deelt de markt voor zoekmachines met Yahoo, Bing en meer niche initiatieven als DuckDuckGo, Wolfram Alpha, Iens en Funda).

Concurrentie is ook cruciaal voor investeringen in internetinfrastructuur. Nederland kent sinds de fusie van UPC en Ziggo twee private aanbieders. De infrastructuur van KPN (koper en glasvezel) moet opengesteld worden voor concurrenten zonder eigen netwerk (zoals Tele2). De infrastructuur van Ziggo (kabel) hoeft dat nog niet. D66 blijft strijden voor een gezonde markt met voldoende spelers waarbij ook de kabel volledig open moet voor concurrenten zonder netwerk.⁴⁶ In Duitsland valt de digitale infrastructuur onder de Infrastructuur-begroting en helpt de overheid in onrendabele buitengebieden. Dat zou in Nederland ook moeten. Ook is het belangrijk gemeentes te helpen bij het vinden van locaties waar warmtekrachtkoppelingen benut kunnen worden voor datacenters. Ook moeten verordeningen die investeringen in nieuwe verbindingen dwarsbomen, geschrapt worden. Ten slotte moet Nederland blijvend investeren in de aanleg van razendsnel mobiel internet, via 5G-technologie.

44 Met de nieuwe Europese privacy richtlijn wordt privacy wetgeving in Europa geharmoniseerd en is de Europese leidend bij het beschermen van de consument.

45 Zie “The end of power” van Moses Naim (2014).

46 Kabinet en Tweede Kamer zijn hier voor, maar de Europese Commissie en de Nederlandse toezichthouder ACM houden dit vooralsnog tegen.

Box8: de deeleconomie door een kritische bril

Digitale platforms brengen vraag en aanbod bijeen en zijn exponenten van de 'nieuwe deeleconomie'. Hoe positief dit kan zijn, laat het Amerikaanse klusplatform Taskrabbit zien: 70% van de aanbieders was voorheen werkeloos. En door te delen, bijvoorbeeld via een app als Peerby, maken we efficiënter gebruik van onze spullen.⁴⁷ Maar zorgt uitwisseling van goederen en diensten door gelijken via digitale platforms nu echt tot vrijere individuen in een duurzamere wereld?

Allereerst is de term misleidend. Het gaat immers om commerciële transacties. En commerciële platforms als Uber en Airbnb verdienen een hoop aan dat delen. De aanbieders op deze platforms zijn ook lang niet altijd 'peers' die diensten uitwisselen maar ondernemingen. Een huis dat het hele jaar door op Airbnb staat, is een hotel; een kok die dagelijks 20 maaltijden verkoopt via Thuisafgehaald een restaurant. Prima, behalve als voor deze ondernemingen andere regels gelden dan voor hun offline tegenhangers. Vals spelen is overigens een vaak gehoord verwijt: ook Google of de internationale hotelboekingsite Booking.com krijgen dit te horen van de concurrentie.

Ten tweede hebben digitale platforms vaak voordeel van de netwerkeffecten waarmee zij alle aanbieders bij elkaar krijgen. Dat geeft ze de mogelijkheid om prijs en voorwaarden te bepalen zonder dat gebruikers een redelijk alternatief hebben. Zo bleken de chauffeurs van taxibemiddelaar UberPop vaak minder te verdienen dan het minimumloon door de lage omzet en de hoge afdracht.⁴⁸ Ook dreigt ongelijkheid. Alleen degenen met bezit profiteren. Airbnb kan huizenprijzen opdrijven waardoor minder vermogenden uit de stad verdwijnen. Zwarte Amerikanen verhuren hun huis gemiddeld voor 12% minder.⁴⁹ En Booking.com zou volgens het Duitse Bundeskartellamt marktverstorende prijsafspraken maken.

Ten derde is de deeleconomie minder duurzaam dan gedacht. Ja, autodelen vermindert volgens het Planbureau voor de Leefomgeving de uitstoot. Maar tegelijkertijd komen er ook producten binnen het bereik van groepen die anders niet van die producten gebruik zouden kunnen maken. En het verpakken, schoonmaken en transporteren van gedeelde spullen is milieubelastend. Naast breed bezongen wordt de deeleconomie dus ook scherp bekritiseerd in een groeiende reeks artikelen en publicaties.

47 Volgens onderzoek van ShareNL is één boormachine per zes huishoudens genoeg. Door het delen van boormachines te vereenvoudigen kan de productie van vijf andere boormachines bespaard worden.

48 <http://www.volkskrant.nl/tech/uberpop-chauffeur-haalt-vaak-minimum-loon-niet~a3823583/>

49 Zie "Digital Discrimination" van Edelman en Luca, Harvard Business School (2014).

Kies voor echte Netneutraliteit

Concurrentie vereist een gelijk speelveld. Cruciaal hiervoor is netneutraliteit, zodat diensten van startups niet achtergesteld kunnen worden op diensten van gevestigde bedrijven. D66 zette dit in de Nederlandse wet. De Europese Unie heeft het principe van netneutraliteit recent afgezwakt omdat verschillende lidstaten hun gevestigde telecomsector wilde beschermen. D66 blijft zich inzetten voor volwaardige Europese netneutraliteit, zoals president Obama in de VS nastreeft.⁵⁰ Naast het waarborgen van netneutraliteit op de zogenaamde *last mile* (van content-dienst naar eindgebruiker via ISP), komt het interconnectienetwerk steeds meer in beeld als de plek waar netneutraliteit moet worden gehandhaafd.⁵¹

Zo snel mogelijk naar één Digitale Markt

Ontwikkelaars of aanbieders betalen vaak in meerdere Europese lidstaten belasting. Daarom vestigde een bedrijf als Amazon zich in Luxemburg, dat een lager btw-tarief op e-boeken had dan de rest van Europa. D66 wil een goed functionerend belastingsysteem voor online diensten en producten. Totdat er één digitale interne markt is, is het nodig een btw-drempel in te stellen voor het afdragen van btw naar andere landen. Daarnaast moet het midden- en kleinbedrijf bij de Mini One Stop Shop⁵² terecht kunnen ongeacht hun product of dienst.

Maar de versnippering beperkt zich niet tot belastingen. Ook consumentenbescherming en privacy-eisen verschillen van land tot land. D66 blijft in Europa hameren op harmonisering en de creatie van één markt, zoals we ook deden bij roaming en netneutraliteit. De regering moet de plannen voor een digitale interne markt van de Europese Commissie niet alleen steunen maar helpen concretiseren en fors aanjagen. Nederland is het land dat hier het meeste bij te winnen heeft. Grenzen mogen handel niet belemmeren, en zeker niet op internet. D66 wil dat Europa leidend is in de wereld door geharmoniseerde en technologie-neutrale wetgeving waarmee consumenten, ondernemers en de creatieve industrie de vrijheid krijgen die nodig is om digitale kansen optimaal te benutten.

Hervorm het intellectueel eigendom...

Het huidige patentsysteem heeft modernisering. Patenten zijn bedoeld om inventiviteit te belonen en kennis te verspreiden⁵³ maar leiden in de praktijk vaak niet tot innovatie.⁵⁴ Te meer omdat patenten door advocaten bewust vaag en moeilijk

50 <http://nos.nl/artikel/2021609-obama-krijgt-zijn-zin-met-netneutraliteit-in-vs.html>

51 <http://computerworld.nl/netwerken/84352-amerika-krijgt--omgekeerde--netneutraliteit>

52 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/zakelijk/btw/zaken-doen_met_het_buitenland/goederen_en_diensten_naar_andere_eu_landen/btw_berekenen_bij_diensten/wijziging_in_digitale_diensten_vanaf_2015/wijziging_in_digitale_diensten_vanaf_2015

53 De houder van een vondst moet deze verplicht met iedereen delen.

54 <http://www.economist.com/news/leaders/21660522-ideas-fuel-economy-todays-patent-systems-are-rotten-way-rewarding-them-time-fix>

geformuleerd worden. In feite zitten we met een systeem waarin patenthouders er alles aan doen om innovatie tegen te houden, tenzij ze er zelf aan verdienen. Hierdoor is het vaak gunstiger een advocaat in dienst te nemen dan een onderzoeker. In de sector van halfgeleiders moet een starter voor 200 miljoen dollar aan licenties kopen voor hij aan de slag kan. Dit leidt tot een situatie waarin 40 tot 90% van alle patenten nooit gebruikt wordt.⁵⁵ Ook zijn veel hedendaagse monopolies gebaseerd op een patent. Dat maakt medicijnen duurder dan nodig. Zo houdt het huidige patentsysteem gevestigde partijen overeind in plaats van het aanzetten tot innovatie.

D66 wil dat patenten worden uitgerust met een 'use it or lose it'-regel, die zorgt dat het patent verloopt wanneer het niet binnen een redelijke tijd op de markt wordt gezet. Daarbij moet het aanvechten van een patent eenvoudiger worden met lagere proceskosten. Verder moeten patenten alleen nog gegeven worden voor echte doorbraken. Een patent voor de 'ronde hoeken' van Apple is onzin. Ten slotte moet de duur van patenten worden teruggebracht. Een patent van 20 jaar is logisch voor een medicijn dat vele jaren onderzoek en testen vraagt, maar is een eeuwigheid in de ICT. De patentduur moet dus samenhangen met de tijd die nodig is om te komen van idee naar product.

...En moderniseer het auteursrecht

Europa heeft baat bij een auteursrecht dat recht doet aan moderne diensten, creatieve industrie en gebruikers. Maar in het tijdperk van computers en internet gelden nog steeds regels uit de tijd van de typemachine. Op online gedeelde informatie kan auteursrecht rusten dat analoog eenvoudig te beschermen was, maar digitaal niet meer. Grensoverschrijdende diensten zoals Spotify en Netflix ervaren het als struikelblok dat ieder land zijn eigen auteursrecht heeft. Grote bedrijven hebben advocatenteams om door deze regel wirwar heen te ploegen. Startups niet.

Geo-blocking is nu een gangbare praktijk in Europa waardoor audiovisuele media buiten de eigen landsgrenzen niet toegankelijk zijn. Zo is Uitzending Gemist voor Nederlanders niet op vakantie in Frankrijk te zien, terwijl hun belastinggeld wel aan die dienst ten goede komt. D66 wil geo-blocking binnen de EU afschaffen. Nederland moet ook voorkomen dat regels voor 'aanverwante' auteursrechten worden ingevoerd in Europa zodat zoekmachines moeten betalen voor korte citaten uit nieuwsartikelen in de zoekresultaten. Dit heeft geleid tot het stoppen van Google News in Spanje en een sterke terugname van bezoekers aan nieuwswebsites in Duitsland. Er is meer juridische zekerheid nodig over auteursrecht. Bijvoorbeeld voor gebruikers van peer-to-peer (P2P) netwerken bij het delen van beschermde werken zoals films en muziek. ISP's moeten een strikt neutraal doorgeefluik zijn en bij de handhaving dus geen

⁵⁵ <http://www.economist.com/news/leaders/21660522-ideas-fuel-economy-todays-patent-systems-are-rotten-way-rewarding-them-time-fix>

gewichtige rol aan de voorkant krijgen. Als bedrijven bepalen wat wel of niet legaal is en daarop actie ondernemen wordt gerechtelijk en democratisch toezicht ondermijnd.

Het intellectueel eigendom moet eigentijdser worden beschermd. Bijvoorbeeld bij hergebruik van muziek/beeldfragmenten op internet zonder winst. D66 wil nieuwe verplichte uitzonderingen voor niet-commercieel user-generated content zoals samengestelde video's en afbeeldingen, en ook voor tekst- en datamining. Bestaande uitzonderingen voor kopieën voor eigen gebruik, parodieën, citeren en incidenteel gebruik moeten in heel Europa gelden. Ook voor bibliotheken, musea en archieven moeten verplichte uitzonderingen worden uitgebreid. Zo kunnen beschermde werken in hun collecties die actief beschermd worden door de rechthebbenden, toch online beschikbaar komen. Bovendien moet de digitalisering en online beschikbaarheid van Europees cultureel erfgoed beter.

Momenteel bestaat er een versnipperd landschap van 28 auteursrechtstelsels in de EU-lidstaten. Door regels gelijk te trekken en te verduidelijken krijgen innovatieve startups de kans om te bloeien en snel te groeien. De eindoplossing is een Pan-Europees auteursrecht, zoals er ook één Europees merkenrecht en contractrecht is. Ondanks de hoge ambities voor één Digital Single Market heeft het plan voor een Single European Copyright vertraging opgelopen. Mogelijke tussenstap naar één Europese licentie of abonnement is de herziening van de Europese kabel- en satelliet richtlijn uit 1993 die collectief beheer voor audiovisuele internetdiensten alsnog mogelijk maakt.⁵⁶ Dit zou het door D66 bepleite radiomodel op internet realiseren.

⁵⁶ Dit is in 2001 tegengehouden door de EU-lidstaten.



Hoofdstuk 2

Technologie in het publieke domein

Technologie en digitalisering veranderen de manier waarop we dingen organiseren. Via apps, games en smart devices kunnen we steeds grotere hoeveelheden data steeds sneller delen en analyseren. Daarbij worden top-down machtsstructuren vervangen door initiatieven van onderaf. Publieke sectoren als onderwijs en zorg moeten actiever gaan inspelen op deze dynamiek. En de overheid moet technologische mogelijkheden beter (doelgerichter!) benutten om onze steden leefbaar te maken, onze democratie te versterken en de eigen dienstverlening te verbeteren.

De maatschappij vraagt steeds meer digitale vaardigheden van burgers. Voor een succesvolle carrière, voor het omgaan met overheidsinstanties en bedrijven en voor sociale interactie. Dit vergt ook iets van het onderwijs. Nu leren kinderen digitale vaardigheden vooral thuis. Maar niet alle huishoudens hebben een computer en niet alle kinderen leren dit uit zichzelf. Dat kan leiden tot een tweedeling tussen kinderen die digi-vaardig zijn en kinderen die dat niet zijn. Tegelijkertijd biedt digitalisering kansen om het onderwijs zelf dynamischer en uitdagender te maken. Bovendien is meer maatwerk mogelijk. Naast basisvaardigheden bijbrengen moeten we mensen specifiek opleiden voor de banen van morgen. Door mensen kennis te laten maken met programmeren en digitale techniek kunnen zij hun talenten op deze gebieden ontdekken en ontwikkelen.

De zorg is de meest persoonlijke overheidsverantwoordelijkheid. Daarbij gaat het vaak om kwetsbare mensen. Digitalisering van de zorg voelt vaak verkeerd. Het beeld van steriele robots en killercomputers past niet bij de helpende hand die zorgbehoevenden nodig hebben. Maar juist binnen de zorg lijkt technologie grote mogelijkheden te bieden. Niet om zorgtaken over te nemen van professionals, maar wel om hen te helpen hun zorgtaken beter en menselijker uit te voeren. De overheid moet innovatie stimuleren met oog voor onwenselijkheden. Een goed voorbeeld is Buurtzorg Nederland. Het verminderen van bureaucratie en hiërarchie wat deze organisatie zo uniek maakt is voor een groot deel mogelijk door digitale technieken.

Digitale technologie verandert ook onze leefomgeving, onze democratie en publieke dienstverlening. Steden worden slim en GeenPeil wist ruim 400.000 digitale handtekeningen te verzamelen voor het referendum. Ook de overheid digitaliseert (DigiD, digitale mailboxen, online formulieren) maar loopt nog ver achter bij het bedrijfsleven, terwijl mensen en bedrijven juist verwachten hun zaken digitaal af te kunnen handelen. Omdat de overheid betrouwbaar moet zijn, is experimenteren met

nieuwe technieken risicovol. Bovendien kampt de overheid met systemen die vaak al tientallen jaren oud zijn en staat –eveneens verouderde- regelgeving vernieuwing in de weg. Bijvoorbeeld door te stellen dat bepaalde stukken per post opgestuurd moeten worden. Toch kan en moet de overheid digitale doorbraken forceren.

Box9: Internetpessimisme⁵⁷

De fundamentele keuzes over de inrichting van onze digitale samenleving hebben consequenties voor onze samenleving als geheel. Het is niet slechts een technische discussie, maar vooral een politieke. We zien een toenemende marktmacht van bedrijven die over big data en geavanceerde algoritmes beschikken. Bedrijven met minder middelen kunnen deze achterstand vrijwel nooit inhalen, waardoor we een tweedeling zullen gaan zien binnen onze economie. Een dergelijke tweedeling zal ook ontstaan onder consumenten: degenen met het geld en de kennis om hun privacy te beschermen zullen over meer vrijheid beschikken dan de consumenten wiens mogelijkheden gestuurd worden door profilering en targetting. Intussen dreigt er banenverlies en meer inkomensongelijkheid als gevolg van automatisering en robotisering. En het gevaar voor burgers komt ook van de overheden zelf, die steeds meer data van ons willen hebben en ingrijpen in de technische werking van het internet.

Deze ontwikkelingen zijn technisch mogelijk maar maatschappelijk onwenselijk. We moeten marktmacht inperken, burgerrechten waarborgen, digitale kloven dichten en het internet open, vrij en veilig houden voor iedereen. Internetpessimisten stellen echter dat dit (voor de overheid) onmogelijk is. D66 is optimistischer over de digitale toekomst en denkt dat de overheid wel degelijk een sleutelrol kan vervullen in het beheersen van de nadelige gevolgen van digitalisering.

Visie 2030: technologie ondersteunt de mens

Publieke sectoren als het onderwijs en de zorg hebben goed ingespeeld op de digitalisering. Het onderwijs levert mensen af die digitaal vaardig zijn en over voldoende technische kennis beschikken. De leerling staat centraal en wordt dankzij onderwijsdata meer op maat bediend. Hetzelfde geldt voor de zorg. Met slimme

⁵⁷ Wie meer wil lezen over de schaduwkanten van het internet verwijs ik graag naar het boek "Internet is niet het antwoord" van Andrew Keen of 'Het Digitale Proletariaat' van Hans Schnitzler (2015).

internettoepassingen worden zorgbehoefte en zorgaanbieder bijeengebracht en zorgt preventie voor lagere zorgkosten. Maar iedereen is en blijft eigenaar van zijn eigen zorgdata en houdt daar volledige controle over. Robotisering helpt in aanvulling op menselijke taken en is geen vervanging. Zo houden mensen meer ruimte over om te doen waar ze goed in zijn: persoonlijke aandacht geven.

De overheid is erin geslaagd technologie succesvol aan te wenden in het publieke domein. In onze slimme steden is de openbare ruimte veiliger, het verkeer beter gespreid en het energieverbruik gedaald. Digitale mogelijkheden worden benut zonder elk apparaat aan te sluiten op internet. De tendens om alsmaar meer gegevens op te slaan is een halt toegevoegd. Bij gegevensopslag toetst de overheid of de opslag in verhouding tot het beoogde doel staat. Digitale dienstverlening heeft de drempel naar de overheid verlaagd. Verouderde systemen zijn verdwenen maar wie dit wil, krijgt hulp bij het digitaal afhandelen van zaken. Zo blijft de overheid toegankelijk en persoonlijk. De overheid heeft geleerd van het verleden en van andere landen en is een effectieve aanbesteder en inkoper van ICT-projecten geworden. Ook de democratie is versterkt. Niet alleen dankzij succesvolle experimenten met online inspraak en digitale burgerraadpleging maar ook omdat na het succes van #GeenPeil steeds vaker referenda plaatsvinden. Anders dan gevreesd is Nederland erin geslaagd om technologie zo in te zetten dat burgers meer grip hebben op hun leven.

Aanbevelingen

Om de kansen van digitalisering in het publieke domein optimaal te benutten, stelt D66 de volgende maatregelen voor:

Stimuleer de ontwikkeling van digitale vaardigheden

Maar liefst 94% van de Nederlandse huishoudens heeft toegang tot internet en 87% van de Nederlanders gebruikt het internet dagelijks.⁵⁸ Digitale vaardigheden zijn vandaag de dag cruciaal. Desondanks leren kinderen vooral thuis hoe ze om moeten gaan met computers en het internet.⁵⁹ Goed onderwijs bereidt kinderen voor op deze digitale wereld. Hoe ga je om met sociale media? Hoe gebruik je het internet om betrouwbare informatie op te zoeken? Hoe bescherm je je online privacy? Goed onderwijs helpt kinderen hun talenten te vinden en te ontwikkelen. Goed onderwijs stelt leerlingen in staat hun weg te vinden op de arbeidsmarkt of om een eigen bedrijf te beginnen. Het huidige ICT-onderwijs schiet hierin te kort.

58 Eurostat 2015 in ECBO, Laaggeletterden: achterblijvers in een digitale wereld.

59 Luyten, Hans, c.s., De relatie tussen leerling- en schoolkenmerken en digitale geletterdheid van 14-jarigen: secundaire analyses op de data van ICILS-2013, Universiteit Twente, augustus 2015.

D66 wil dat kinderen op de basisschool en middelbare school les krijgen in digitale vaardigheden. Naast enorme kansen kent het internetrisico's op het gebied van privacy en veiligheid. Door kinderen op school digitale vaardigheden te leren kunnen zij de digitale wereld beter begrijpen en er verstandig mee omgaan. Daarbij is kennismaken met programmeren belangrijk om talent te ontwikkelen en probleemoplossend te leren denken. Bovendien kan het kinderen helpen een baan te vinden of een bedrijf te starten. Vrijwel alle grote internetbedrijven hebben één of meerdere oprichters die kunnen programmeren. Denk aan Jeff Bezos (Amazon), Sergey Brin en Larry Page (Google), Mark Zuckerberg (Facebook), Bill Gates (Microsoft) of Elon Musk (Paypal, Tesla, SpaceX). Om lessen in digitale vaardigheden en programmeren mogelijk te maken, zijn leraren met deze vaardigheden nodig. Daarom moeten digitale vaardigheden en programmeren onderdeel worden van de lerarenopleidingen.

Uiteraard is programmeren niet het enige ingrediënt. D66 wil meer aandacht voor ondernemerschap op hogescholen en universiteiten. Het kenmerk van startups is dat ze snel inspringen op nieuwe technologische ontwikkelingen en dat maakt deze bedrijven essentieel voor onze toekomstige welvaart. Dat betekent dat we onze knapste koppen hierin moeten trainen. Waarbij het bijbrengen van overige academische kennis van groot belang blijft: grote innovators stonden vaak op de scheidslijn van techniek en de kunsten of geesteswetenschappen.⁶⁰ Ook veel volwassenen willen leren coderen: meer dan 24 miljoen mensen hebben gebruik gemaakt van de gratis lessen van op de site van Codeacademy en het Amerikaanse '*Hour of Code*' heeft al meer dan 28 miljoen mensen overgehaald programmeren eens te proberen.⁶¹ Mensen die hun baan kwijtraken als gevolg van automatisering moeten worden ondersteund bij herscholing voor de digitale wereld. Hier ligt ook een mooie rol voor bibliotheken die van origine centra van kennisdeling zijn.

Stel de leerling centraal via digitaal onderwijs

Een digitale wereld vraagt nieuw onderwijs. We zien steeds meer tablets, laptops en digibords in de klas, wat het leergemak van kinderen vergroot en het makkelijker maakt hun voortgang te volgen. Daarnaast biedt *gamification* de mogelijkheid om van leren een speelse aangelegenheid te maken, wat blijkt uit de populariteit van sites als DuoLingo. Naast technische ondersteuning in de les, zien we ook dat traditionele lessen vervangen worden door online kanalen. Leerlingen leren steeds vaker zelfstandig via MOOCs (massive open online courses), apps, of Youtube colleges. Dit biedt mogelijkheden om rekening te houden met de interesses en snelheid van de individuele leerling. Aan aanbod geen gebrek meer en zo kan voor ieder kind een eigen lesprogramma opgesteld worden.

60 Zie "The Innovators" van Walter Isaacson (2014).

61 The New York Times, 23 March 2014, "Adding Coding to the Curriculum".

Lang draaide het onderwijs rond de leraar als absolute autoriteit en bron van kennis. Diens rol blijft doorslaggevend, maar meer als begeleider. Met technologie en data kunnen we het beste uit iedere leerling halen, maar daar moet het onderwijs dan wel op ingericht worden. Dat betekent in de eerste plaats: erop vertrouwen dat de leraar het beste kan inschatten wat de leerling (of diens ouders) nodig heeft en niet de leergang dichttimmeren met vaste trajecten. Daarnaast moet het makkelijker worden om on- en offline methodes te combineren. Ook voor resultaten die niet op één school behaald zijn, maar bijvoorbeeld op een online platform als Coursera. Een leerling kan dan een breder profiel bouwen en is niet afhankelijk van de vakken die op zijn of haar school worden aangeboden.

Ten slotte biedt interpretatie van data de mogelijkheid om online methodes beter en sneller (in principe real-time) te ontwikkelen dan traditionele, offline lespakketten. Ook kunnen dergelijke data de noodzaak tot toetsing verminderen, aangezien de voortgang van een leerling continu gevolgd kan worden. D66 ziet potentie in deze ontwikkeling voor verbetering van het onderwijs, maar alleen onder de voorwaarde dat dergelijke persoonsdata de privacy van de leerling niet schaadt. Het is belangrijk dat de leerling uiteindelijk eigenaar blijft van zijn data en bepaalt wat hiermee gebeurt.

Met robots naar menselijke zorg

Ook in de zorg worden robots steeds meer toegepast. Zo is al succes geboekt met hulp van robots bij operaties. Naast geavanceerde machines die ondersteuning bieden bij mechanische ingrepen, worden robots ook gebruikt als vervanging voor menselijk contact, bijvoorbeeld in de ouderenzorg. Robots kunnen ingezet worden voor verzorging maar ook om vereenzaming tegen te gaan.⁶² De voordelen hiervan gaan verder dan alleen 'lagere kosten'. In specifieke gevallen kan contact met een robot voorkeur hebben boven menselijk contact. Denk aan hulp bij het douchen of naar het toilet gaan. De documentaire "Ik ben Alice"⁶³ liet mooie resultaten zien en onderzoek wijst uit dat mensen genegenheid kunnen voelen voor apparaten. Of het eenzaamheid tegengaat moet nader worden onderzocht op basis van empirische data. Met het oog op hogere zorgkwaliteit en zelfstandigere patiënten is D66 voorstander van meer onderzoek naar, en experimenten, met robots in de zorg.

Intussen staan innovatiebudgetten onder druk van de decentralisatie van de zorg. Er moeten daarom nieuwe bronnen van financiering voor (onderzoek naar) innovatieve zorgtoepassingen worden aangeboord. Hiertoe moeten we robotbehandelingen beter verzekeraar maken en gericht vrij geld maken voor medische innovatie. Daarnaast moeten we belemmeringen in verouderde regelgeving wegnemen en actief op zoek gaan naar oplossingen voor nieuwe vraagstukken. Wie is er bijvoorbeeld verantwoordelijk wanneer een robot een fout maakt?⁶⁴

62 Vrij Nederland 25 maart 2015, "Robot Alice en mevrouw Van Wittmarschen".

63 Kijk 'Ik ben Alice' via uitzending gemist: http://www.npo.nl/2doc/06-07-2015/KN_1671620

64 Een grappig experiment met een huishoudrobot wordt beschreven in een artikel in FD Outlook "Onze robot heeft schade gereden: wie betaalt dat?".

Stel de patiënt centraal via technologie in de zorg

Digitale toepassingen hebben hun weg gevonden naar de zorgsector. We kunnen onze gezondheid met zelfmeetapparatuur steeds beter monitoren – van hartslag en suikerspiegel tot stressniveau en slaapgedrag. Dit leidt tot nieuwe inzichten en meer voorspelbaarheid van ziekte. Tegelijkertijd zijn er berichten over artsen die foto's van patiënten doorsturen via WhatsApp⁶⁵ of verzekeraars die gegevens kwijtraken.⁶⁶ We moeten voorkomen dat ethische dilemma's de mogelijkheden van zorg en data in de weg staan. Waar de zorg van oudsher een offline en publiek georiënteerd domein was, groeit nu de rol van digitale, private ondernemers. Mensen zoeken zelf naar een diagnose op commerciële websites, laten hun gezondheid meten door een app en bestellen medicijnen bij een online apotheek. Maar we reguleren de zorgmarkt niet voor niets. Hoogwaardige gezondheidszorg is een teken van beschaving en mensen met een zorgvraag zijn kwetsbaar. Bij private partijen ligt het gevaar op de loer dat commerciële belangen die van de patiënt overschaduwden. D66 wil daarom dat private partijen, net als in andere sectoren, aan hun zorgtaak gehouden worden.

De rol van de arts verandert door de groeiende beschikbaarheid van medische informatie. De patiënt stapt met meer informatie de wachtkamer binnen, waardoor de arts in de toekomst meer tijd kan besteden aan behandeling en preventie mits de zelfdiagnose juist is.⁶⁷ De les uit de digitalisering van de media is dat meer data een groeiende behoefte aan interpretatie geeft.⁶⁸ Bij de zorg kunnen computers wellicht helpen met de diagnose maar uiteindelijk zal een arts de beslissing moeten nemen. D66 wil dat artsen de zo vrijkomende tijd investeren in de relatie met de patiënt. Daar komt bij dat de arts steeds minder de hoofdbewaarder van medische informatie zal zijn. We moeten voorkomen dat het monopolie van artsen over patiëntdata wordt ingeruild door een monopolie van private partijen. De patiënt moet daarom volledige controle houden over zijn of haar medische gegevens met de mogelijkheid deze in te zien en eventueel te verwijderen. Zonder goede beveiliging en harde privacy waarborgen kunnen meer medische gegevens onze zorg niet beter maken.

Centrale dataopslag lijkt logisch maar alle commotie rond het elektronisch patiëntendossier (EPD) heeft aangetoond hoe moeilijk dit ligt, ook al is een papierendossier evenmin onfeilbaar en toekomstbestendig. D66 stelt daarom een persoonlijk zorgdossier voor waarbij burgers zelf kunnen kiezen tussen verschillende aanbieders binnen de door de overheid vastgestelde kaders. Dat kan een bedrijf zijn, een groep artsen en zorgverleners zoals Whitebox,⁶⁹ of een open source oplossing van

65 Elsevier 27 september 2013, "Artsen gebruiken onveilig WhatsApp voor patiëntenfoto's".

66 Financieel Dagblad 7 maart 2015, "Gezocht: data over mijn dokter".

67 De Tijd 28 maart 2015, "Een dokter in je broekzak"

68 Voor nieuwsfeiten is de ouderwetse journalist niet meer nodig. Daarentegen groeit de vraag naar opiniemakers en duiding.

69 <https://www.security.nl/posting/442854/Huisartsen+ontwikkelen+nieuw+Elektronisch+Pati%C3%ABnten+Dossier>

vrijwilligers. Dit moet gebeuren met open standaarden voor de opslag en uitwisseling van data zodat alle gebruikers ermee kunnen werken. Daarnaast moeten er duidelijke protocollen zijn over de uitwisseling van data en overheidscontroles op de systemen. Zo kan iedereen een systeem kiezen dat bij hem past. Dat dit gaat ten koste van de beschikbaarheid van de gegevens in een noodgeval, is acceptabel mits de patiënt er bewust voor gekozen heeft privacy te verkiezen boven medische noodzaak.

Geef patiënten inzicht in de zorgkwaliteit

Zorgverzekeraars, dokters en wetenschappers beschikken over enorme hoeveelheden data. Als deze discreet geanalyseerd worden, geeft dat patiënten meer inzicht en kan de kwaliteit van de zorg beter vergeleken worden. Bovendien kunnen deze gegevens leiden tot kostenbesparingen en dus lagere zorgpremies. D66 wil daarom alle zorgdata beschikbaar maken als open data.

Naast informatie over patiënten wordt ook steeds meer bijgehouden over artsen. In Nederland kunnen patiënten hier nauwelijks informatie over krijgen. We vertrouwen blindelings op de doorverwijzing van onze huisarts, wat meestal leidt tot behandeling in het dichtstbijzijnde ziekenhuis. Op de site zorgkaartnederland.nl kunnen mensen hun ervaringen met artsen en instellingen delen, maar dit is geen volledige en objectieve informatie. In de VS geeft de site betterdoctor.com een overzicht van specialisten in de omgeving, informatie over hun opleiding, hun tarieven, welke verzekering hun behandeling vergoedt en recensies van eerdere patiënten.⁷⁰

Medische data zijn vaak lastig te interpreteren. Zo is het aantal overlijdensgevallen bij hartoperaties in een ziekenhuis afhankelijk van meer variabelen dan enkel de kunde van de arts en de faciliteiten van de instelling. De informatie moet niet gebruikt worden om individuele artsen te beoordelen maar kan wel worden ingezet bij de keuze voor een zorgaanbieder. In Nederland vertrouwen we deze regierol voornamelijk toe aan de zorgverzekeraar. De vraag is echter of die het best in staat is om de individuele belangen van de patiënt te behartigen. Het gevaar bestaat daarnaast dat het niet ontsluiten van zorgdata ertoe leidt dat patiënten op anekdotische basis informatie gaan uitwisselen. Juist gezien de complexiteit van medische data zou dat ongewenst zijn.

Zet in op slimme steden maar blijf realistisch

De wereld verstedelijkt. Ook in Nederland is het percentage Nederlanders dat in een gemeente met meer dan 100.000 inwoners leeft sinds 1980 gestegen van 26,8% naar 35,64%.⁷¹ Steden zijn economische, sociale en culturele motoren waar vraag en aanbod van goederen, diensten, kennis, nieuwe ideeën en mensen samenkomen. Maar hoe groter een stad, des te complexer de organisatie van verkeer, huisvesting,

⁷⁰ Financieel Dagblad 7 maart 2015, "Gezocht: data over mijn dokter.

⁷¹ Cijfers CBS

energie- en watervoorziening en afvalverwerking. Deze groeiende complexiteit kunnen we te lijf gaan met het slim toepassen van het Internet of Things en Big Data.⁷² Zo krijgen we 'Smart Cities' waarin 'real-time informatie' problemen helpt oplossen. Een voorbeeld is het stadsdashboard dat de gemeente Rotterdam in de strijd tegen roet en fijnstof. Op basis van gekoppelde data over het lokale verkeer, geluid, kadastrale gegevens en luchtkwaliteit kunnen beleidsmakers betere keuzes maken. Een andere mogelijke toepassing is slimme verlichting die zich door een koppeling van systemen aanpast aan de aanwezigheid van mensen in een deel van de stad.

Ook deze data moeten voor iedereen beschikbaar zijn, om het creatieve potentieel van alle ondernemers en bewoners te benutten. De toenemende invloed op de eigen omgeving zal de sociale betrokkenheid vergroten. Wel moeten reële risico's als hacks, privacyschending en invloedrijke algoritmes worden onderkend. Als multinationals al moeite hebben om hackers buiten te houden, zal het voor een kleine gemeente nog lastiger zijn. En er zijn goede waarborgen nodig om te voorkomen dat de verzamelde data herleidbaar zijn tot individuen. Omdat er geen 'opt-out' is voor burgers, moeten Smart Cities geen speeltje van beleidsmakers worden.⁷³ De oplossing van een stedelijk probleem moet centraal staan, realisme en zorgvuldigheid moeten leidend zijn en de belangen van de burgers moeten ermee gediend worden.

De overheid moet daarom een regierol nemen, de juiste kaders scheppen en zorgen voor goede controle. Onder leiding van Ron van der Lans van de Amsterdam Economic Board trok onze hoofdstad de regierol actief naar zich toe en is daarmee uitgegroeid tot een toonaangevende Smart City. Ook Den Haag timmert flink aan de weg.⁷⁴ D66 wil slimme steden stimuleren. Waar nationale regels in de weg staan, zoals de aanbestedingsregels, moeten we deze moderniseren.

Versterk de democratie door digitalisering

Digitalisering biedt mogelijkheden voor versterking van de democratie. Maar het contrast tussen de huidige systemen en de verwachtingen van burgers groeit. Terwijl je via je smartphone een vakantie kunt bestellen of een verzekering kunt afsluiten, is ook onze laatste democratische innovatie, het referendum, (deels) een papieren proces. Zonder voorbij te gaan aan betrouwbaarheid, kijkt D66 naar drie digitale mogelijkheden om onze democratie te versterken.

⁷² TNO, Agenda voor Nederland.

⁷³ Zo laat Singapore zien dat manipulatie via Smart City-data (inclusief gezichtsherkenning, straatsensoren en het aftappen van social media en smartphones!) een reëel risico vormt. Ook China gaat ver in het laten gehoorzamen van burgers via het datasysteem Sesame Credits. Verder vormen gehackte steden, overmachtige bedrijven, falende overheden en oncontroleerbare algoritmen een gevaar voor de positie van burgers.

⁷⁴ Zie: "Kansen voor Groei, ICT Klimaat in Den Haag en Haaglanden", Dr. E.J. de Vries (2013).

Allereerst door meer transparantie: digitalisering maakt het delen van overheidsdata makkelijker en vergroot het inzicht in activiteiten van de overheid. Dat vergroot de mogelijkheid om mee te doen aan besluitvorming en controle op de uitvoering ervan. Dat kan gaan van het beschikbaar stellen van de bouwtekeningen van het buurtpleintje tot het beschikbaar stellen van de stemgegevens van de Tweede Kamer. Door data pro-actief (dus niet pas na een verzoek) te delen heeft de overheid niet meer het alleenrecht op de informatie. Ten tweede: via een betere dialoog. Waar in een “papier democratie” het aantal contactmomenten met de kiezer beperkt is, biedt digitalisering de mogelijkheid om het contact te intensiveren. Dankzij Twitter is de directe aanspreekbaarheid van politici toegenomen. Maar ook meer inhoudelijk zijn er mogelijkheden. Een gedurfd voorbeeld hiervan is IJsland die in 2012 een grondwet aannam die middels “crowdsourcing” was opgesteld.⁷⁵ Ten derde: verbetering van het electorale proces zelf. De invulling van onze democratie is niet significant gewijzigd de afgelopen eeuwen terwijl digitalisering de wereld eromheen wel drastisch veranderd heeft. Omdat betrouwbaarheid en nauwkeurigheid bovenaan staan, is het terecht dat we niet halsoverkop nieuwe innovaties doorvoeren. Maar ook de papieren stembethode is niet zonder fouten of nadelen. Geleidelijke digitalisering biedt kansen om nieuwe voordelen gecontroleerd te introduceren. Dit kan leiden tot een hogere ‘opkomst’ en een sneller en goedkoper proces.

Experimenteer met digitale dienstverlening

Nederland is voor veel private partijen een digitale proeftuin maar onze overheid loopt achter met digitale dienstverlening. Daarom is het zaak dat ondernemers en burgers vanaf 2017 al hun zaken met de overheid digitaal kunnen regelen. Daarbij kunnen we leren van een land als Estland en moet experimenteren makkelijker worden. Tijdelijke uitzonderingen op regels moeten -mits gepast en zonder rechtszekerheid te schaden- mogelijk zijn om een digitale aanpak uit te proberen. Zo kan de Belastingdienst met een kleine groep ondernemers (beta-testers) een nieuwe manier van BTW-aangifte uitproberen voordat dit beschikbaar komt voor alle ondernemers. Klein beginnen, leren van fouten en dan uitbreiden, is de te volgen strategie.

Omdat digitale dienstverlening het gebruiksgemak kan vergroten en kosten kan verlagen wil D66 dit verbeteren en uitbreiden maar zonder mensen buiten te sluiten die niet mee willen of kunnen komen. Zo’n 6% van Nederland is digibeet en veel van deze mensen zijn, door een uitkering of een andere reden, juist afhankelijk van de overheid.⁷⁶ Daarom moet het begrip voor laaggeletterdheid binnen de rijksoverheid vergroot worden bij de omgang met burgers, door systemen voor digitaal-laaggeletterden zo gebruiksvriendelijk mogelijk te maken. Daarbij, juist omdat het merendeel van de dienstverlening automatisch afgedaan kan worden, ontstaat er

⁷⁵ <http://www.wired.co.uk/news/archive/2012-10/23/iceland-crowdsourced-constitution>

⁷⁶ ECBO, “Laaggeletterden: achterblijvers in de digitale wereld?” (2015).

ruimte voor medewerkers om de extra service te verlenen die nodig is. In plaats van het tegen hoge kosten aanhouden van niet-digitale kanalen (zoals de blauwe enveloppe van de Belastingdienst) is D66 voorstander van meer gemeentelijke dienstverlening aan huis.⁷⁷ Zo kan een medewerker van de gemeente aan huis assistentie bieden bij bijvoorbeeld het aanvragen van toeslagen.

Ook moet de overheid actiever digitale technologieën omarmen. Neem bijvoorbeeld Bitcoin, of liever de achterliggende technologie: de Blockchain technologie. Deze kan ook de dienstverlening van de overheid verbeteren. Alleen al het uitkeren van toeslagen kost €200 miljoen euro en daar komt nog eens €100 miljoen aan fraude bij. Met Blockchain zou dit efficiënter kunnen en kan fraude voorkomen worden door de digitale munteenheid te programmeren voor een bepaald doel. Zorgtoeslag kan dan bijvoorbeeld alleen aan zorg worden uitgegeven.

Meer realisme en betere organisatie van ICT-projecten

Voor betere digitale dienstverlening zijn goede informatiesystemen een randvoorwaarde. De commissie ICT-projecten liet zien dat ICT-projecten bij de overheid vaak verkeerd verlopen.⁷⁸ D66 onderschrijft de verbetervoorstellen zoals andere aanbestedingsprocedures, het voorkomen van een vendor-lock-in, een onafhankelijk Bureau ICT Toetsing (BIT) en meer kennis van ICT voor ambtenaren. Daarnaast wil D66 dat de overheid kiest voor open source software en open standaarden waar mogelijk, zodat publiek gefinancierde software zoveel mogelijk publiek beschikbaar is. Daarnaast omdat openbare code ontwikkelaars een prikkel geeft om goed werk te leveren en omdat het zo eenvoudiger is om nieuwe partijen oude software te laten door ontwikkelen.

De overheid is een grote klant en heeft veel invloed in de Nederlandse markt. Maar de recente geschiedenis van ICT-aanbestedingen is geen gelukkige. Vaak speelt de overheid gevestigde partijen in de hand doordat aanbestedingen alleen op het lijf van grote partijen zijn geschreven. D66 wil dat overheidsopdrachten beter toegankelijk worden voor kleinere partijen, bijvoorbeeld door ICT-projecten op te knippen of door coöperatieve platformen te faciliteren. Dit breekt de markt open voor kleine partijen en verkleint de afhankelijkheid van één enkele leverancier. De overheid moet fundamenteel anders naar ICT projecten gaan kijken. Het idee dat een systeem tot in de puntjes beschreven kan worden om dan in een meerjarenproject gebouwd te worden blijkt vaak een droom. In het bedrijfsleven is daarom “Agile-softwareontwikkeling” in opkomst.⁷⁹ Dit is anders dan de traditionele watervalmethode omdat het eindproduct niet vast ligt. In plaats daarvan wordt zeer snel een basaal maar bruikbaar product opgeleverd (ook wel een Minimum Viable Product genoemd). Op basis van gebruikerservaringen

77 <http://www.ingovernment.nl/artikelingovernment/reisdocumenten-thuis-op-het-werk-bezorgd>

78 <http://www.tweedekamer.nl/kamerleden/commissies/tcict>

79 <http://www.agilemanifesto.org/>

wordt die in vaste, elkaar snel opvolgende intervallen doorontwikkeld totdat het aantal overeengekomen uren of budget is bereikt.⁸⁰ Dit vereist een totaal andere manier van opdrachtgeverschap. D66 wil deze aanpak uitproberen in het publieke domein door er bij één of meerdere uitvoeringsinstanties proeven mee te doen.

Hoe dan ook is uitbreiding van ICT-kennis bij overheden nodig. Zoals de overheid ook niet alle juridische kennis van buiten haalt, kan dit ook niet langer voor ICT-kennis. Leveranciers zijn het erover eens dat de overheid een slechte ICT-opdrachtgever is, omdat inhoudelijke kennis en sturing bij ambtenaren ontbreekt. D66 pleit ervoor dat de overheid kennis over ICT en opdrachtgeverschap structureel gaat opbouwen.

Maak technologie tot kabinetsprioriteit via een minister van Economie, Technologie en Privacy

De toenemende invloed van internet en technologie op economie en samenleving rechtvaardigen een meer centrale positie in het beleid en de organisatie van de Rijksoverheid. Dit kan niet door het te beleggen bij één enkel beleidsdepartment of het benoemen van een digi-commissaris. In het eerste geval isoleer je het beleid. In het tweede geval is meer samenhang wel mogelijk, maar is er te weinig daadkracht. Analoot aan de bestaande sociaal-economische zeshoek,⁸¹ kiest D66 daarom voor een “digitale driehoek”, waarbij drie ministeries het kloppend hart vormen van integraal kabinetsbeleid om de kansen en uitdagingen van technologie het hoofd te bieden.

Allereerst wil D66 een ministerie van Economie, Technologie en Privacy dat enerzijds nieuwe technologie stimuleert en anderzijds waakt over eerlijke concurrentieverhoudingen en de persoonlijke levenssfeer in het digitale domein. De mededingingswet, de wet bescherming persoonsgegevens en de algemene wet gelijke behandeling vormen het kader dat gehandhaafd wordt door de Autoriteit Consument en Markt (ACM) en de Autoriteit Persoonsgegevens (AP). Het tweede ministerie in de driehoek is het ministerie van Binnenlandse Zaken dat verantwoordelijk is voor de binnenlandse veiligheid en de gebundelde inkoop en aanbesteding van ICT. Hier zijn de CTIVD en het BIT de onafhankelijke toezichthouders. Het derde ministerie is Justitie, verantwoordelijk voor de rechtstaat, opsporing en cyberveiligheid in Nederland. Met het NCSC als onafhankelijke waakhond.

80 Het Verenigd Koninkrijk loopt hierin voorop via de in 2011 opgerichte Government Digital Services van de Britse overheid. Een nieuwe overheidswebsite stond binnen 10 weken online. De besparingen worden geschat op 200 miljoen pond. En premier Cameron zei hierover: “I believe the creation of the Government Digital Service is one of the great unsung triumphs of the last Parliament”.

81 De ministers van Economische zaken, Financiën, Sociale Zaken, Binnenlandse zaken, Welzijn, Volksgezondheid en Cultuur en de minister-president. Zij vormen een van de onderraden van de Ministerraad, waarin de belangrijkste financieel-economische beslissingen worden gemaakt.

Box10: Wat kan Nederland leren van andere landen?

- Estland zet in op digitalisering van hun samenleving: burgers staan in contact met de overheid met digitaal stemmen, een digitale identiteitspas (en “digitaal burgerschap”!) en een portal voor alle overheidszaken. Er is daarnaast veel aandacht voor start-ups.⁸²
- IJsland heeft een “crowdsourced” grondwet waarbij burgers op verschillende (digitale) wijzen konden meeschrijven: hoewel geen doorslaand succes wel een leerzaam voorbeeld.⁸³
- In het Verenigd Koninkrijk is programmeren sinds 2014 onderdeel van het vaste lespakket: vanaf vijf jaar oud krijgen kinderen op alle scholen hun eerste programmeerervaring met simpele logica tot het leren van een “echte” programmeertaal rond hun twaalfde.⁸⁴
- In Estland leren kinderen op de meeste scholen al vanaf zesjarige leeftijd programmeren en ook Australië, Nieuw-Zeeland, Israël, Denemarken⁸⁵, Finland, en sinds kort ook België⁸⁶ hebben (in de nabije toekomst) vergelijkbare initiatieven in basis- of middelbaar onderwijs.
- Israël is een “startup powerhouse”: naar rato van inwoners beginnen er de meeste tech-startups ter wereld.⁸⁷
- In Duitsland valt de digitale infrastructuur onder het ministerie van Transport: in perifere gebieden zorgt de overheid voor goede internetverbindingen.
- De Verenigde Staten kunnen mensen alle arts objectief vergelijken dankzij de website betterdoctor.com.
- België heeft al sinds 2003 (!) een elektronische identiteitskaart op het formaat van een bankkaart en met een chip.

82 <http://tegenlicht.vpro.nl/afleveringen/2014-2015/e-stonia.html>

83 http://www.slate.com/articles/technology/future_tense/2014/07/five_lessons_from_ice-land_s_failed_crowdsourced_constitution_experiment.2.html

84 <http://www.theguardian.com/technology/2014/sep/04/coding-school-computing-children-programming>

85 The Economist, 26 April 2014, “A is for Algorithm”.

86 <http://tweakers.net/nieuws/102288/vlaamse-academies-willen-dat-alle-kinderen-leren-programmeren.html>

87 http://www.economist.com/node/17796932?story_id=17796932

Hoofdstuk 3

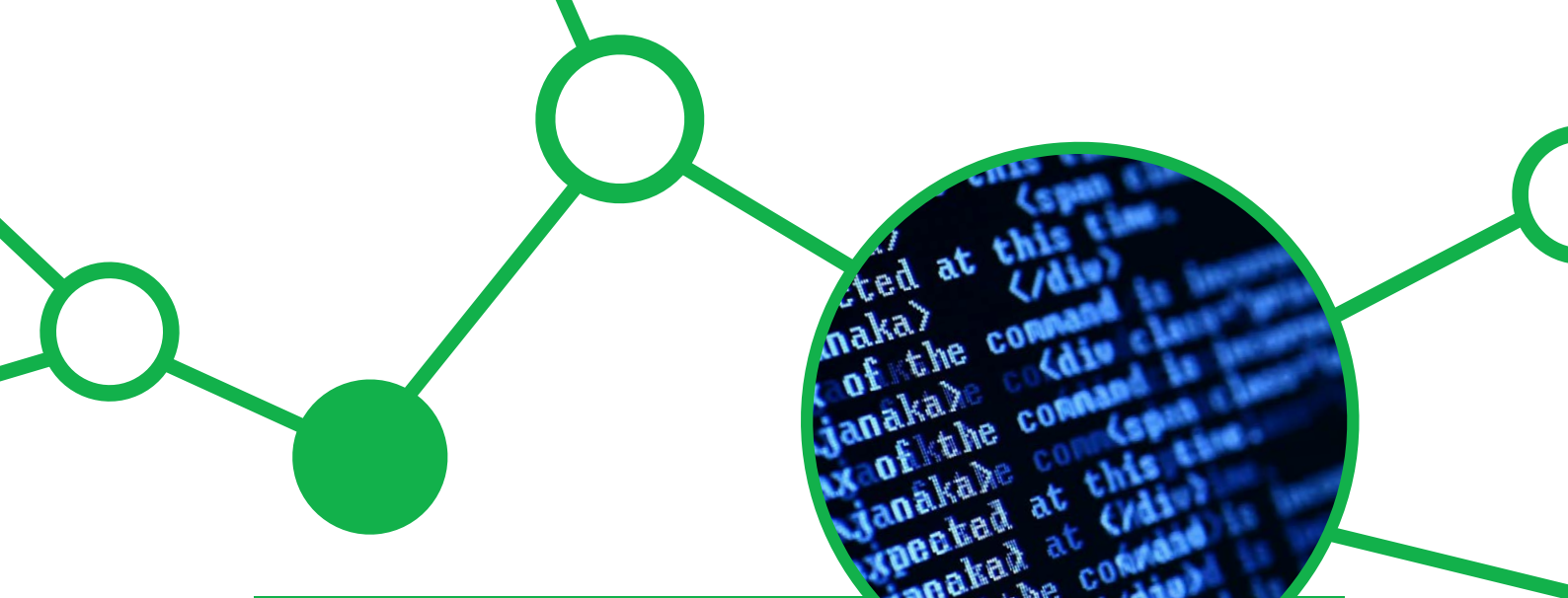
Online vrijheid

Vrij en open internet stelt mensen in de gelegenheid om informatie te vergaren, hun mening te uiten en zich persoonlijk te vormen. In tegenstelling tot bijvoorbeeld China is de online bewegingsvrijheid in Nederland onbeperkt. Maar vanzelfsprekend is dat niet. Met de komst van krachtigere computers en snellere internetverbindingen creëren, verzamelen en gebruiken burgers, bedrijven en overheden meer digitale informatie dan ooit tevoren. Zo wordt voortdurend bijgehouden wat we zoeken, kopen, *liken*, lezen of versturen. We laten niet alleen zelf digitale sporen achter maar ook via posts, tags en foto's van vrienden en collega's. Je 'digitale footprint' wordt zo je digitale schaduw. Overheden en bedrijven verzamelen grote hoeveelheden data. Dit roept niet alleen vragen op over onze privacy (wie weet wat van mij?) maar raakt ook steeds meer aan het recht op gelijke behandeling (welke behandeling hoort bij mijn profiel?).

De hoeveelheid data wordt namelijk niet alleen groter, de analyse ervan wordt ook steeds geavanceerder. Informatie die afzonderlijk nutteloos was, kan in combinatie met andere databases een goudmijn blijken (en tevens zeer persoonlijke informatie onthullen!). Algoritmes scannen diverse databestanden tegelijkertijd en trekken daaruit pijlsnel conclusies over het gedrag van consumenten (*profiling*). Op basis van deze profilering krijgen bepaalde consumenten specifieke aanbevelingen of aanbiedingen (*targeting*). Waar men vroeger bij het adverteren zich richtte op doelgroepen heeft men nu de mogelijkheid om gericht informatie te sturen naar individuen. Profilering kan dus voordelen opleveren maar heeft als gevaar dat onjuiste conclusies worden getrokken of dat groepen personen worden uitgesloten.⁸⁸ Ook al zijn algoritmes rekenregels, dat maakt ze nog niet neutraal of objectief. Er zitten allerlei bewuste en onbewuste aannames in verwerkt die de bouwer veel meer macht geven dan de consument.

Veel mensen zijn zich niet bewust van deze privacy-risico's en of mogelijke informatiesturing en zelfs datadiscriminatie. Omdat dit raakt aan onze persoonlijke ontwikkeling en de vrijheid van het individu, moeten we vooral bij kinderen waakzaam zijn voor de negatieve gevolgen. Al vanaf jonge leeftijd surfen zij op het web en laten ze een digitale voetafdruk achter. Omdat online alles wordt geregistreerd, zijn fouten snel fataal en komt hun vrije ontwikkeling onder druk.

88 'De rechtsstaat in cyberspace?' – Inaugurele rede door Prof.mr.dr. M. Hildebrandt van de Radboud Universiteit Nijmegen.



Box11: Voorbeelden van profiling

Bedrijven misbruiken geregeld hun informatiemacht. Google gebruikte data om gepersonaliseerde advertenties te tonen, zonder vooraf de gebruiker te informeren of om toestemming te vragen. In 2014 legde het College Bescherming Persoonsgegevens Google een last onder dwangsom af, die kon oplopen tot 15 miljoen euro. In datzelfde jaar werd ook bekend dat Facebook berichten op de newsfeed van meer dan 700.000 profielen heeft ‘verstoppt’ om te toetsen of de getoonde emotie in statusupdates besmettelijk is.

Maar het zijn niet alleen de techgiganten die zich schuldig maken aan informatiesturing. Zo bleek dat uitzendbureaus Randstad en Adecco medische gegevens verzamelden van uitzendkrachten die zich ziek meldden en deze gegevens langer bewaarden dan noodzakelijk. Uit een ander onderzoek van het CBP bleek dat Snappet, een aanbieder van tabletonderwijs, in strijd met de wet handelde door leerresultaten van kinderen te gebruiken voor vergelijkingsonderzoek zonder dat scholen hiermee hadden ingestemd. En advertentiebedrijf YD (inmiddels: Yieldr) verzamelde zonder toestemming persoonsgegevens via tracking cookies, om gepersonaliseerde advertenties te tonen.

In 2012 publiceerde The New York Times een spraakmakend artikel over het gebruik van big data door de Amerikaanse winkelketen Target. Een vader was woest geworden op een manager in een van de winkels, nadat zijn tienerdochter waardebonnen had ontvangen voor babykleertjes en wiegjes. Hij beschuldigde de winkel ervan haar aan te moedigen zwanger te worden. Maar Target bleek meer over de tiener te weten dan haar eigen vader: ze was namelijk al in verwachting. De winkelketen had een algoritme ontwikkeld om via aankoopdata en online zoekgedrag te voorspellen of een klant zwanger was...

Visie 2030: Een open en vrij internet dat niet stiekem ingrijpt in onze levens

Ook online kan iedereen veilig en vrij communiceren. Mensen zijn en blijven eigenaar van hun persoonsgegevens, ook als ze die –bewust of onbewust- delen via internetdiensten en social media bedrijven. Zowel bedrijven als overheidsinstellingen geven inzicht in de data die ze verzamelen, hoe ze die gebruiken en wat de gevolgen zijn voor de gebruiker. Doelbinding tot het strikt noodzakelijke staat altijd centraal en er wordt streng toegezien op naleving van grondrechten en de gelijke behandeling van alle consumenten. Gegevens zijn zowel bij de overheid als het bedrijfsleven goed beveiligd door encryptie en privacy by design. Het open internet zorgt dat we vrijelijk onze mening kunnen geven en zonder beperkingen informatie kunnen vinden. We hebben vertrouwen in de werking en veiligheid van het internet. Nederland is een internationale voorvechter van een open en vrij internet, stimuleert encryptie wereldwijd en zet zich in voor de bescherming van het internet als mondiaal publiek goed.

Aanbevelingen

Om het internet open en vrij te houden en de privacy en gelijke behandeling van internetgebruikers te garanderen, speelt de overheid een cruciale rol. Daarom pleit D66 voor de volgende maatregelen:

Geef dominante internetbedrijven een zorgplicht

De bescherming van burgers tegen de datamacht internetbedrijven gebeurt met meerdere wetten. Centraal staat de wet bescherming persoonsgegevens (Wbp).⁸⁹ Daarnaast is er de wet bescherming gelijke behandeling die (data)discriminatie moet voorkomen. Maar het is ook een kwestie van mededinging en consumentenbescherming. Naast het informeren van burgers moet de overheid bedrijven daarom ook aanspreken op hun zorgplicht. Zoekbedrijven, webwinkels en *social media* diensten zijn in de afgelopen jaren uitgegroeid tot semi-nutsbedrijven.⁹⁰ Hun alomtegenwoordigheid en de grote informatie-asymmetrie ten opzichte van gebruikers geeft hen een grote verantwoordelijkheid. Minister Kamp (EZ) wil een uitbreiding van de zorgplicht van aanbieders, maar heeft hier nog geen concreet vervolg aan gegeven.⁹¹ Zoals de

89 De huidige Wbp is gebaseerd op de Europese Privacy Richtlijn uit 1995. Na vaststelling (2016) en inwerkingtreding (2018) van de nieuwe Europese privacyverordening (de Algemene Verordening Gegevensbescherming en de daarvan afgeleide Europese Richtlijn voor Politie en Justitie) moet de Wbp hierop worden aangepast: <http://www.recht.nl/nieuws/privacyrecht/140918/de-vijf-belangrijkste-punten-uit-de-nieuwe-europese-privacyverordening/>.

90 Andrew Keen noemt in "Internet is niet het Antwoord" als meest dominante voorbeelden van haast onvermijdelijke systeembedrijven Google, Amazon en Facebook. Dave Eggers geeft een schets van een almachtig internetbedrijf dat alles van iedereen wil weten in zijn bestseller "The Circle" (2013). Dat is fantasie maar megawebshop Alibaba, zoekmachine Baidu en berichtenapp WeChat laten zien dat dit in China al bijna werkelijkheid is. China voert in 2020 een "Sociale kredietwaarde" in: een op vele digitale data gebaseerde score die de betrouwbaarheid van mensen en bedrijven weergeeft!

91 Stichting Digitale Infrastructuur Nederland, "Visie op de relatie Internet en Overheid" (2014).

zorgplicht banken verplicht hun klanten gedegen te informeren over financiële markten en producten, wil D66 dat technologiebedrijven gebruikers ook op een duidelijke manier openheid geven over alle verzamelde gegevens en de beveiliging ervan.

Naast deze transparantie moeten bedrijven consumenten actief en laagdrempelig laten weten wat er met hun gegevens gebeurt. De privacy-voorwaarden van veel bedrijven zijn nu vaak onleesbaar en zo lang dat het lezen meer tijd kost dan met het daadwerkelijke internetgebruik.⁹² Door consumenten kort en goed te informeren (via icoontjes of infographics) weten consumenten waar ze aan toe zijn en kunnen ze weloverwogen keuzes maken.

Encryptie en privacy by design spelen een belangrijke rol, die alleen maar belangrijker wordt met het uitdijende Internet of Things. Echter, voor bedrijven zijn de voordelen van technische maatregelen (cryptotechnologie, transparantietools, etc.) of organisatorische maatregelen (functionarissen voor gegevensbescherming, pseudoniemen, audits, etc.) moeilijk meetbaar. En bij het inbouwen van privacy by design als standaard gaan de kosten vaak voor de baten uit. Door sterkere handhaving op privacy- en cybersecuritymaatregelen zijn deze investeringen sneller commercieel aantrekkelijk. Hiertoe kan de overheid privacy by design actiever stimuleren, bijvoorbeeld via voorlichting, certificering en de eigen inkoop.

De zorgplicht is vooral noodzakelijk voor dominante spelers met een economische machtspositie. Mededingingsinstanties moeten deze controleren ter bescherming van de consumentenvrijheid. Naast een Europese aanpak (zoals Google nu ondervindt), wil D66 het budget van de ACM vergroten, zodat het effectief kan handhaven op onwenselijke netwerkeffecten.⁹³ Daarnaast beperkt strenge doelbinding de impact van dataverzamelingen. In de Europese verordening is doelbinding echter onderuit geschoven: verder werken met de data voor een ander doel is toegestaan, zolang het een legitiem belang van het bedrijf is. D66 wil een hardere garantie van doelbinding zonder ruime uitzonderingsgronden.

92 Financieel Dagblad 29 november 2014: Interview Natali Helberger “Personaliseren sites leidt tot manipulatie”.

93 De mededingingswet volstaat op zich in het digitale domein, alleen is handhaving in de praktijk lastiger geworden. Door het internet zijn er steeds meer gevallen waarbij één speler heel snel, heel dominant kan worden. Hier moet de mededingingsautoriteit goed tegen opgewassen zijn. Overigens wist de ACM hier zelf ook op in hun uitgave ‘Het Signaal 2015’ (pagina 2 t/m 5).

Box12: Belangrijke wetgeving die het internet raakt⁹⁴

- Europees Verdrag voor de Rechten van de Mens (EVRM): verdrag tot bescherming van de rechten van de mens en fundamentele vrijheden.
- Verdrag 108 van de Raad van Europa voor de bescherming van individuen met betrekking tot de automatische verwerking van persoonlijke gegevens: verdrag over de verwerking van persoonsgegevens.
- Handvest van de Grondrechten van de Europese Unie: handvest met de grondrechten van burgers binnen de EU.
- Europese richtlijn gegevensbescherming 95/46/EG: Europese richtlijn uit 1995 over de verwerking en het gebruik van persoonsgegevens. Deze moet zorgen dat in alle lidstaten dezelfde regels omtrent privacy gelden, waarbij het gaat om alle gegevens die herleidbaar zijn tot personen. De richtlijn wordt binnenkort vervangen door de Algemene Verordening Gegevensbescherming (AVG).⁹⁵
- Network and Information Security directive (NIS): Europese richtlijn voor netwerk en informatiebeveiliging.
- Wet bescherming persoonsgegevens (Wbp): deze wet waarborgt, zowel online als offline, zorgvuldige omgang met persoonsgegevens. Met name artikel 13 in de Wbp is van belang, aangezien dit artikel stelt dat bedrijven en overheden ervoor dienen te zorgen dat de beveiliging van hun elektronische bestanden op orde is. De huidige Wbp zal komen te vervallen bij inwerkingtreding van de nieuwe Europese privacyverordening, de AVG.
- Algemene wet gelijke behandeling (Awgb): deze wet bevat algemene regels ter bescherming tegen discriminatie op grond van godsdienst,

94 Toezicht op de naleving van deze wetten gebeurt door onafhankelijke organen zoals het College voor de Rechten van de Mens, de Autoriteit Persoonsgegevens (voorheen College bescherming persoonsgegevens, CBP), of de Autoriteit Consument en Markt (ACM).

95 De Algemene Verordening Gegevensbescherming (AVG) bevat de basisregels voor de verwerking van persoonsgegevens door bedrijven én overheden. Een deel van de verordening behoeft nationale implementatie in wetgeving, onder meer om er voor te zorgen dat de in te stellen toezichthouder de benodigde bevoegdheden wordt toegekend. In aanvulling op de AVG wordt een richtlijn vastgesteld voor de verwerking van persoonsgegevens door politie en justitie bij de opsporing en vervolging van strafbare feiten. Deze zal worden geïmplementeerd in de opvolger(s) van de Wet politiegegevens en de Wet strafvorderlijke en justitiële gegevens.

levensovertuiging, politieke gezindheid, ras, geslacht, nationaliteit, hetero- of homoseksuele gerichtheid of burgerlijke staat.

- De Telecommunicatiewet (Tw): bevat regels rondom telecommunicatie. Zowel netneutraliteit als de zogenaamde cookiewet maken hiervan onderdeel uit.
- Wet Computer criminaliteit III: wetsvoorstel dat opsporingsdiensten toestaat binnen te dringen in geautomatiseerd werk.
- Wet op de Inlichtingen en Veiligheidsdiensten (Wiv): wetsvoorstel dat inlichtingendiensten in staat stelt ongericht kabelgebonden internetverkeer te onderscheppen.
- Wet Bewaarplicht Telecommunicatiegegevens: Deze wet verplichtte internet- en telefoonaanbieders gegevens over internet- en telefoniegebruik voor zes tot twaalf maanden te bewaren, zodat veiligheidsdiensten dit konden gebruiken in de bestrijding van terrorisme. Op 11 maart 2015 is de wet buiten werking gesteld, wegens schending van enkele artikelen in het Europees Handvest voor de rechten van de mens. Een nieuw wetsvoorstel om de bewaarplicht te regelen is in consultatie gegeven door het kabinet, maar nog niet ingediend bij de Kamer.

Informeer gebruikers over de werking van algoritmes

Mensen beleven privacy online anders dan in de fysieke wereld. We geven zonder aarzeling onze contactgegevens bij bestellingen via webshops, maar tonen achterdocht wanneer een winkelmedewerker onze postcode vraagt.⁹⁶ Om het bewustzijn te vergroten moet de overheid zorgen dat bedrijven transparanter zijn over de opslag en het gebruik van gegevens. Inzicht in algoritmes is hierbij onmisbaar. De online ervaring en beleving van mensen wordt namelijk in grote mate bepaald door algoritmes:⁹⁷ rekenregels die op basis van profielen pagina A of pagina B tonen na een zoekopdracht. Dat dit grote invloed kan hebben, blijkt uit een recente studie van het American Institute for Behavioral Research and Technology die laat zien dat de uitslag van een verkiezing tot 25% kan worden beïnvloed door algoritmen van zoekmachines als Google.⁹⁸

96 Financieel Dagblad, 10 januari 2015, "*Retailer weet in 2030 precies hoe de klant door de winkel reist*".

97 In dit kader wordt vaak gesproken van de Filter bubble waarbij algoritmen op basis van persoonlijke profielen selecteren welke informatie de gebruiker waarschijnlijk wil zien.

98 <http://www.wired.com/2015/08/googles-search-algorithm-steal-presidency/>

Hierbij gaat het niet om de algoritmes zelf maar om de gevolgen ervan,⁹⁹ zoals het bij de bijsluiter van medicijnen ook niet gaat om bestanddelen maar om mogelijke bijwerkingen. Voor algoritmes met een grote impact op onze privacy en online behandeling moet een bijsluiter komen die consumenten informeert over het effect.¹⁰⁰ Zo hoeft het algoritme zelf niet gedeeld te worden, wat de concurrentiepositie van (Nederlandse) bedrijven ten goede komt.

Zodra consumenten weten welke gevolgen rekenregels kunnen hebben, begrijpen ze beter hoe hun online behandeling tot stand komt. Het helpt ook beseffen wat allemaal mogelijk is met hun gegevens. Als een paar keer te laat betalen bij een webwinkel leidt tot het profiel 'mogelijke wanbetaler' en die gegevens gedeeld worden met een autodealer, kan het bijvoorbeeld moeilijker worden een auto op krediet te kopen. Meer bewustzijn van deze mechanismen geeft consumenten de gelegenheid keuzes te maken in hun online handelen. Overigens zijn algoritmes niet foutloos. Zo nam een computersysteem van een Amerikaanse universiteit aan dat promovendi uitsluitend mannen zouden zijn en zag een ander algoritme een dansende mensenmassa aan voor een beginnende vechtpartij en belde de politie.¹⁰¹

Voorkom datadiscriminatie van consumenten

Er ontstaat een steeds groter spanningsveld tussen profilering en informatiesturing enerzijds, en gelijke behandeling anderzijds.¹⁰² Volgens de Algemene wet gelijke behandeling (art 7 Awgb) heeft iedereen recht op gelijke behandeling bij de toegang tot goederen en diensten, zonder onderscheid op grond van geloof, huidskleur, geslacht, nationaliteit of seksuele geaardheid. In profilering via big data en algoritmes is dit onderscheid er vaak wel degelijk. Bedrijven willen niet direct onderscheid maken, maar indirect gebeurt het wel. De wet laat ook ruimte voor uitzonderingen wanneer bedrijven onderscheid rechtvaardigen in het belang van commerciële doelen.¹⁰³ Zo valt het onderscheid in verzekeringspremies op basis van leeftijdscategorie niet onder prijsdiscriminatie. Nu het steeds makkelijker wordt om met behulp van algoritmes onderscheid te maken, is het belangrijk om scherp te blijven op gelijke behandeling. Bovendien moeten consumenten weten of ze dezelfde prijs aangeboden krijgen als anderen. Sommige webwinkels proberen

99 De wiskundige regels van een algoritme zeggen de gemiddelde consument immers nog minder dan een lange tekst van een gebruiksaanwijzing.

100 Dit is ingewikkelder in het geval van machine learning algoritmes, een automatisch lerend systeem, waarbij de maker zelf ook geen inzicht heeft in de werking ervan. In dat geval kan inzicht gegeven worden in het doel van het machine learning algoritme en de informatie die als input ervoor gegeven wordt.

101 <http://www.dailymail.co.uk/news/article-3000705/Female-paediatrician-locked-gym-changing-room-computer-assumed-Doctor-title-MAN.html>

<http://www.nrc.nl/nieuws/2015/08/22/hoe-de-politie-misdaad-opspoort-nog-voordat-die-heeft-plaatsgevonden>

102 Kamerstuk 32761 nr. 78 – Verwerking en bescherming persoonsgegevens

103 Kamerstuk 32761 nr. 78 – Verwerking en bescherming persoonsgegevens

namelijk in te schatten hoeveel de bezoekers kunnen besteden en passen daar de prijs van hun producten op aan.¹⁰⁴ In dat geval is de discriminatie geen onbedoeld gevolg van profilering, maar een bewuste tactiek voor meer winst.

De overheid heeft een rol in het voorkomen van manipulatie en datadiscriminatie. Naast het inzichtelijk maken van de werking van algoritmes, is de volgende stap het aanpassen van regelgeving in verschillende vakgebieden om gelijke behandeling te garanderen.¹⁰⁵ We zien echter dat de datadiscriminatie verder gaat dan de toegang tot goederen en diensten. Er is ook discriminatie in de privacy die consumenten geboden wordt. Zo heeft Achmea consumenten korting geboden op hun premie als zij kastjes in hun huis en auto plaatsen om hun gedrag te meten.¹⁰⁶ Mensen die minder te besteden hebben doen zoiets eerder dan vermogende mensen. Maar iets essentieels als privacy mag niet alleen te koop zijn. Uiteraard geldt dit ook voor een deel van de gegevens die gratis webdiensten als Facebook of Google verwerken. De overheid moet daarom randvoorwaarden bewaken, zodat voor iedereen, ongeacht hun vermogen, een minimumniveau van privacy beschikbaar is. Gezien de nauwe samenhang die dit heeft met de wet bescherming persoonsgegevens, is het logisch het toezicht hierop bij de Autoriteit Persoonsgegevens te leggen.

Geen data verzamelen zonder expliciete toestemming

Data zijn het nieuwe geld.¹⁰⁷ Aan het begin van deze eeuw zijn internetbedrijven begonnen met het heimelijk verzamelen van data over personen voor commercieel gebruik (gerichte advertenties). De belangrijkste techniek voor dit nieuwe verdienmodel zijn cookies, kleine bestandjes die een website op je computer zet die je surfgedrag bijhouden en die door derden kunnen worden uitgelezen. De consument was zich hier niet van bewust, had dus geen enkele keuze en is ook nooit om toestemming gevraagd. In Europa leidde dit tot een maatschappelijk debat over de wenselijkheid van het online volgen van consumentengedrag. In Nederland nam de Tweede Kamer in 2012 de cookiewet aan, die gebruikers een expliciete keuze moest geven (wel of geen cookies accepteren). De praktijk was echter pop-ups met veel irritatie en weinig keus omdat veel websites alleen toegankelijk bleven voor mensen die cookies accepteerden. Ook de ‘weloverwogen toestemming’ zoals bedoeld in art. 11.7a van de Telecommunicatiewet, die een vertaling vormt van de Europese Privacyrichtlijn, bleef uit.¹⁰⁸

104 <http://lifehacker.com/5973689/how-web-sites-vary-prices-based-on-your-information-and-what-you-can-do-about-it>

105 Financieel Dagblad 29 november 2014, Interview Natali Helberger “Personaliseren sites leidt tot manipulatie”.

106 Financieel Dagblad 1 oktober 2015, “Achmea geeft premiekorting aan klant die data levert”.

107 Zoals de Autoriteit Persoonsgegevens schrijft in het Jaarverslag 2015: “Apps, zoekmachines, sociale media: zij worden vaak alleen nog tegen betaling met persoonsgegevens aangeboden. Persoonsgegevens worden zodoende vermarkt. Geld wordt op deze terreinen als ruilmiddel langzaamaan vervangen door persoonsgegevens.”

108 Kamerstuk 32761 nr. 78 – Verwerking en bescherming persoonsgegevens

Wel heeft de cookiewet het bewustzijn onder internetgebruikers vergroot, met als gevolg dat steeds meer mensen gebruik maken van technieken om niet gevolgd te worden, zoals browser-plugins of een Virtual Private Network (VPN). Los van de volgtechnologie die bedrijven inzetten, wil D66 het bewustzijn van mensen over online volgen vergroten (ondanks het mogelijke *chilling effect*¹⁰⁹). Ook wil D66 dat mensen altijd een keuze wordt geboden en expliciete toestemming vereist is voor het verwerken van gegevens door derden. Browser-plugins (zoals Ghostery en Disconnect) geven mensen volledige controle over welke cookies zij per website willen accepteren. In plaats van de huidige cookiewetgeving wil D66 daarom dat mensen via de browser toestemming geven voor online volgtechnieken. Alleen dan is sprake van een echte keuze, omdat mensen per website kunnen kiezen welke cookies ze toelaten en het vergroot het gebruikersgemak doordat de keuze geautomatiseerd wordt.

Tegenwoordig zijn steeds meer bedrijven dataverzamelaars. Te denken valt aan autofabrikanten, zorgapparatuur en zelfs leveranciers van software in slimme steden. Belangrijk uitgangspunt is daarom dat gebruikers van deze producten en diensten eigenaar van hun data blijven.

Laat mensen hun gegevens inzien en waar nodig aanpassen of wissen

Ook nadat de gebruiker toestemming heeft gegeven voor het verzamelen van persoonsgegevens, moeten deze data te allen tijde zijn eigendom blijven.¹¹⁰ Deze gegevens mogen dus niet zonder toestemming van de consument worden gedeeld of doorverkocht. Ook moeten mensen kunnen inzien welke gegevens van hen bekend zijn en vervolgens kunnen afdwingen dat foutieve of problematische gegevens gecorrigeerd of zelfs gewist worden.

Het Europese Hof van Justitie heeft in 2014 de uitspraak gedaan dat iedere EU-burger het recht heeft om 'vergeten' te mogen worden.¹¹¹ Maar met de zaak van Google Spain versus Mario Costeja is deze discussie over het recht op het verwijderen van online gegevens nog niet afgedaan. In een tijd waarin *stranger shaming* aan de orde van de dag is, zoals ook weer bleek met het filmpje van de 'terrasmeisjes',¹¹² moet de mogelijkheid bestaan om informatie snel te verwijderen. Soms wordt er al in korte tijd zoveel schade berokkend, dat het verwijderen van de bron nog maar weinig zin heeft.

Meer budget en capaciteit Autoriteit Persoonsgegevens

Bedrijven gaan een verantwoordelijkheid aan zodra zij informatie van hun klanten of derden opslaan. Denk aan inlog-, adres-, of betalingsgegevens. Met een stijgende

109 Dit gebeurt wanneer mensen niet langer vrij communiceren omdat ze bang zijn digitale sporen na te laten. Angst over schending van privacy kan immers net zo verlamdend werken als de daadwerkelijke schending ervan. Zie ook: Kamerstuk 32761 nr. 78 – Verwerking en bescherming persoonsgegevens.

110 Volgens de nieuwe Europese dataprotectie verordening is de definitie van een persoonsgegeven de volgende: "iedere informatie betreffende een betrokkene" http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_nl.pdf.

111 Volkskrant 13 mei 2014, "Recht om vergeten te worden?: reden voor een feestje?".

112 Algemeen Dagblad 8 juli 2015, "Terrasmeisjes durven de deur niet uit na gefilmde ruzie".

kans dat bedrijven gehackt worden moeten organisaties niet alleen voorkomen dat data gehackt wordt, maar ook verantwoordelijk handelen zodra ze gehackt zijn. Bedrijven realiseren zich dat diefstal van persoonsgegevens serieuze gevolgen kan hebben voor het vertrouwen. Daarom ondernemen ze actie om de kans op digitale inbraken en hun impact te minimaliseren. Steeds vaker komen bedrijven zelf naar buiten met data-lekken om hun klanten te informeren.

Omdat dit niet voor iedere organisatie vanzelfsprekend is, bestaan er twee meldplichten: één bij het Nationaal Cyber Security Centrum (NCSC) voor digitale veiligheidsincidenten binnen zes vitale sectoren. En één bij de Autoriteit Persoonsgegevens: sinds 1 januari 2016 moeten organisaties melding maken van “ernstige” datalekken maar alleen als dit leidt tot “ernstige nadelige gevolgen voor de bescherming van persoonsgegevens”.¹¹³

De Autoriteit Persoonsgegevens is nu de kleinste markttoezichthouder, terwijl persoonsgegevens gezien worden als het nieuwe geld waar we de ‘gratis’ internetdiensten mee betalen. Bovendien moet de Autoriteit zowel de publieke als de private sector controleren en zijn de taken van de Autoriteit Persoonsgegevens uitgebreid door de aanstaande privacyverordening van de EU.¹¹⁴ Omdat de hoeveelheid werk van de Autoriteit Persoonsgegevens sterk stijgt,¹¹⁵ vindt D66 dat haar budget verdriedubbeld moet worden naar €25 miljoen in 2020.¹¹⁶ Ook wil D66 dat organisaties een datalek voortaan in alle gevallen moeten melden, ook als er nog geen schade is. Daar moet tegenover staan dat overheden meldingen alert en accuraat afhandelen.¹¹⁷

Voorkom dat schijnveiligheid onze vrijheid inperkt

Ook de overheid verzamelt steeds meer data. De angst voor aanslagen maakt dat veel politici oproepen tot steeds meer veiligheidsmaatregelen, meestal in de vorm van het inwinnen van extra informatie. Zo stelt het kabinet vier wetten voor om de bevoegdheden voor opsporingsdiensten en inlichtingen- en veiligheidsdiensten fors te verruimen. Het wetsvoorstel computercriminaliteit III geeft de politie een hackbevoegdheid en de wet op de inlichtingen en veiligheidsdiensten (Wiv) moet de AIVD en de MIVD gelegenheid geven ongericht kabelgebonden verkeer af te tappen. Ook wil het kabinet de wet bewaarplicht (voor het bewaren en inzien van bel- en internetverkeer) opnieuw invoeren nadat het Europees Hof een streep heeft gezet door -de hieraan ten grondslag liggende- richtlijn dataretentie omdat deze in strijd zou zijn met grondrechten. Tot slot hebben de Europese Commissie, de Europese

113 <https://www.cbppweb.nl/nl/melden/meldplicht-datalekken>

114 <http://ec.europa.eu/justice/data-protection/>

115 Zo heeft het CBP de afgelopen jaren vaker handhavend opgetreden op basis van artikel 13 van de Wet bescherming persoonsgegevens (wbp) tegen beveiligingslekken en onzorgvuldigheden in de private en publieke sector.

116 Dat dit geen overbodige luxe is, bleek ook in België: daar bond de Privacycommissie (50fte) vorig jaar de strijd aan met Facebook (8.348fte).

117 Bijvoorbeeld door gebruik te maken van een goed follow-up protocol.

Raad en het Europees Parlement in december een pakket aangenomen waarbij een database van reis- en passagiersgegevens wordt geregeld (PNR).

Deze voorstellen hebben als doel het vergroten van veiligheid maar kennen belangrijke nadelen: Allereerst is het slecht voor de privacy. Het op grote schaal – ongericht – opslaan van persoonsgegevens (een sleepnet) is door het Europees Hof bestempeld als een ontoelaatbare schending van de privacy en als inbreuk op de fundamentele rechten van Europese burgers. Ten tweede schaadt het de economie. Er is een brede coalitie van grote en kleine bedrijven en bedrijvenclubs die zich herhaaldelijk tegen deze wetten keren omdat grote internetbedrijven en startups liever elders gaan zitten als de overheid zomaar in hun klantdata kan kijken.¹¹⁸ Ten derde maakt dit het internet onveiliger doordat de overheid een belang krijgt, via hackbevoegdheden, bij kwetsbaarheden in software van op het internet aangesloten apparaten. Ten slotte, en dat is het belangrijkste probleem, werkt het gewoon niet. Steeds is de noodzaak en de effectiviteit van een grotere databerg niet duidelijk en evenmin is gebleken dat de aanslagen met deze maatregelen voorkomen hadden kunnen worden.¹¹⁹ Vaak blijkt achteraf dat de nodige informatie over daders van terroristische aanslagen wel aanwezig was maar niet goed behandeld werd. De oud technologie directeur van de Amerikaanse nationale veiligheidsdienst NSA, Bill Binney, stelde zelfs dat bulkdata levens kosten!¹²⁰

Daarom pleit D66 voor het beter en gericht benutten van bestaande bevoegdheden door in te zetten op samenwerking en vooral verplichte informatie-uitwisseling door inlichtingendiensten. Deze cruciale stap is ook na de aanslagen in Parijs niet gezet. Daarbij dienen er ook betere waarborgen te zijn voor bescherming van de rechten van burgers die geen verdachte zijn. Maatregelen dienen toetsbaar te zijn op noodzaak en proportionaliteit. Belangrijk zijn goede rechterlijke toetsing vooraf en scherp (onafhankelijk!) toezicht achteraf door een onafhankelijke toezichthouder op de inlichtingendiensten (de CTIVD)¹²¹ met voldoende – dus extra! – capaciteit. En als er dan data verzameld worden moeten ook zaken als bewaartermijn en toegang strak geregeld zijn. Ten derde is het zaak te investeren in “human intelligence” in plaats van massa surveillance.

118 In 2014 schreven een grote groep internet/technologiebedrijven en branches een gezamenlijk position paper over hun zorgen over de hackwet: KPN, Vodafone, Ziggo, TomTom, Google, Microsoft, AMS-IX, Nederland ICT, Hostingbedrijven, Datacenters, etcetera.

119 Volkskrant 6 maart 2014, Bart Jacobs: “Nieuwe spionagewet bij voorbaat achterhaald”.

120 <http://www.independent.co.uk/life-style/gadgets-and-tech/news/bill-binney-the-snoopers-charter-is-going-to-kill-people-ex-nsa-technical-director-and-whistleblower-a6799156.html>

121 De uitgave “Ten standards for oversight en transparency of national intelligence services” (Instituut voor Informatierecht, Universiteit van Amsterdam, 2015) biedt hiervoor uitstekende aanknopingspunten. Hierbij moet ook de rol en de werkwijze van de Commissie voor de Inlichtingen- en Veiligheidsdiensten (“Commissie Stiekem”) betrokken worden.

Box13: De publieke kern van het internet

De Wetenschappelijke Raad voor het Regeringsbeleid heeft in 2015 een rapport gepubliceerd genaamd 'de publieke kern van het internet'. Daarin worden aanbevelingen gedaan over de rol van overheden op het internet. Zo zouden centrale protocollen en infrastructuur (zoals het TCP/IP protocol suite, verschillende standaarden, het systeem van domeinnamen (DNS) en routing protocollen) gevrijwaard moeten zijn van bemoeienis van overheden. Het rapport stelt dat 'het internet als publiek goed alleen functioneert als het de kernwaarden universaliteit, interoperabiliteit en toegankelijkheid garandeert en de kerndoelen van informatieveiligheid, te weten vertrouwelijkheid, integriteit en beschikbaarheid ondersteunt.' Het internet open en vrij houden is essentieel om het vertrouwen van burgers te behouden in zowel de technische werking van het internet, als de sociaal culturele en economische systemen die ervan afhankelijk zijn.

Encryptie als grondrecht

Cryptografische bewerkingen zoals *encryptie* en *hashing* beschermen vertrouwelijke gegevens. Encryptie is het versleutelen van data zodat de gegevens onleesbaar zijn voor derden. Hashing maakt van informatie een unieke hashcode en deze techniek wordt veel gebruikt voor wachtwoorden.¹²² Sterke encryptie is essentieel voor de bescherming van onze digitale infrastructuur en communicatie, en daarmee niet alleen belangrijk voor onze democratische vrijheid maar ook van groot economisch belang. Het beschermt gevoelige persoonsgegevens, bedrijfsgeheimen en overheidsbelangen, en bemoeilijkt (economische) spionage. D66 wil dat de overheid de ontwikkeling en toepassing van sterke encryptie stimuleert. Eind 2015 is daartoe een amendement van D66 aangenomen waarmee €500.000 geïnvesteerd wordt in open source encryptie projecten. Dit versterkt ook de internationale concurrentiepositie van Nederland. Een land dat het gebruik van sterke encryptie stimuleert, heeft een aantrekkelijk vestigingsklimaat voor bedrijven die afhankelijk zijn van sterke beveiliging van gevoelige informatie en communicatie en bedrijven die de data van gebruikers veilig willen opslaan. Afnemers zullen er altijd voor kiezen hun gevoelige informatie onder te brengen bij bedrijven die hoogwaardige encryptie toepassen.

Ook internationaal moet Nederland werk maken van het versterken van cryptotechnologie. Bovendien moet de overheid zich onthouden van (wettelijke)

¹²² Beide technologieën leiden niet tot anonimisering (identificatie van de persoon wiens gegevens het betreft is nooit meer mogelijk), maar tot pseudonimisering (identificeerbare gegevens worden vervangen door andere gegevens). Het is omkeerbaar (decryptie), herhaalbaar (oorspronkelijke gegevens kunnen meerdere keren opnieuw versleuteld worden) en zorgt ervoor dat gegevens niet gelezen kunnen worden als het in verkeerde handen terecht komt.

beperkingen die de ontwikkeling en toepassing van hoogwaardige encryptie in de weg staan, zoals het stellen van grenzen aan de maximale lengte van encryptiesleutels, het bewust inbouwen van ingangen ten behoeve van de overheid (zoals *backdoors*), of het verplicht toevoegen en afstaan van extra sleutels. Op verzoek van D66 heeft het kabinet een brief geschreven over encryptie waarin het standpunt wordt toegelicht dat Nederland voorstander is van sterke encryptie software. Dit had weer invloed op de discussie in Frankrijk.¹²³ Een andere (automatische) opsporingsmethode waar de overheid zich verre van moet houden, is Deep Packet Inspection (DPI): soft- en hardware die de inhoud van internetverkeer eerst inziet alvorens deze bij de ontvanger aankomt. Ook hier geldt dat burgers zo bij voorbaat als verdachte behandeld worden: onwenselijk dus.

Na de uitspraak van het Europees Hof over Safe Harbor barstte de discussie over de veiligheid van data van Europese burgers in de Verenigde Staten los: de afspraken tussen de Europese Unie en de Verenigde Staten konden niet garanderen dat Amerikaanse inlichtingendiensten niet bij de data konden. Sterke encryptie is dan nog de enige oplossing om mensen zekerheid te bieden omtrent de veiligheid van hun data. Overigens valt na de onthullingen van Edward Snowden uit 2013 over het enorme datasleepnet van de Amerikaanse veiligheidsdienst NSA een hoopgevende trend te ontwaren: private bedrijven als Apple (versus de FBI), Google en Whatsapp (versleuteling) en Twitter (het sluiten van de datasluis (de dienst Dataminr) voor de Amerikaanse justitie) werken hier niet meer stilzwijgend of schoorvoetend aan mee maar nemen maatregelen om klantdata beter te beschermen.

Laat als overheid zien welke data je verzamelt en gebruikt

Naast het bedrijfsleven is de overheid zelf ook een steeds grotere verzamelaar en gebruiker van persoonsgegevens. Vaak zijn burgers verplicht deze data af te geven dus moet er met grote zorg mee omgegaan worden. Zo moet altijd duidelijk zijn welke gegevens bij de overheid bekend zijn, welke instantie ze heeft ingezien en/of ze kan gebruiken. Een land dat hierin ver vooruit loopt, is Estland. Esten hebben op een succesvolle manier inzicht via het programma X-road. Naast het inzien van hun eigen gegevens kunnen ze deze ook corrigeren waar nodig. X-road maakt ook strenger toezien op misbruik van gegevens mogelijk. Zo werden twee verpleegkundigen ontslagen nadat ze onterecht het medisch dossier van een politicus hadden bekeken.¹²⁴ D66 vindt dat de Nederlandse overheid tekort schiet in het geven van inzicht in gegevensgebruik.¹²⁵ D66 pleit ervoor dat Nederlanders net als Esten via een programma als X-road goed inzicht krijgen in de opslag van hun gegevens en het

¹²³ <http://www.numerama.com/politique/137054-les-pays-bas-livrent-un-plaidoyer-en-faveur-du-chiffrement-fort.html>

¹²⁴ Marieke Vos in iBestuur: "De Esten doen het beter" (december 2014).

¹²⁵ Via mijn.overheid.nl kan je weliswaar inzien welke gegevens bij welke overheidsinstantie bekend zijn maar niet wat ermee gebeurt.

gebruik ervan. Dit is niet voldoende om al het wantrouwen weg te nemen. Dit blijkt wel in het geval van identiteitsfraude bij DigiD: de burger is zelf verantwoordelijk voor het aantonen van de fraude, terwijl het systeem door de overheid is opgelegd. Naast sterke beveiliging is het daarom belangrijk dat er net zulke sterke mogelijkheden voor detectie en herstel achteraf bestaan in het geval van ongeautoriseerde toegang door fraudeurs. Alleen op deze manier kunnen burgers erop vertrouwen de volledige controle te hebben over hun eigen gegevens.

Privacy by Design: beperk basisregistraties en bestandenkoppeling

Ook de overheid kan meer gebruik maken van 'privacy by design'. TNO hanteert de volgende definitie:¹²⁶ *"Privacy by Design heeft als doel privacyschendingen zoveel mogelijk te vermijden door privacybescherming vanaf het begin van een (business) proces waar verzameling en verwerking van persoonsgegevens onderdeel van uitmaakt en tijdens de gehele levenscyclus van de gegevensverwerking systematisch 'in te bakken' in de organisatie en in de informatiesystemen die gebruikt worden. Het gaat bij Privacy by Design niet alleen om de technische maatregelen maar ook om maatregelen in de bedrijfsvoering en de organisatie en om inbreng van de ervaring en houding van eindgebruikers (consumenten)."*

Voor de overheid betekent dit allereerst dat het opeisen van allerlei informatie begrensd moet worden. Nederland kent inmiddels maar liefst twaalf basisregistraties (die met elkaar verbonden worden in een stelsel waarbinnen alle reeds bekende informatie met verschillende overheidsinstanties wordt gedeeld)¹²⁷ Ook buiten dit stelsel is meer terughoudendheid nodig bij het koppelen en uitwisselen van gegevensbestanden en datasets tussen diverse publieke instanties (van lokaal tot nationaal). Fraudeaanpak mag geen legitimatie van eindeloze koppeling zijn. Verder moet privacy by design de standaard worden bij ICT-aanbestedingen van zowel software als hardware.

Strijd wereldwijd voor een open en vrij internet

De ontwikkeling en het beheer van het internet waren lange tijd vooral een technische exercitie waar overheden slechts in beperkte mate bij betrokken waren. Beslissingen over *hoe* het internet werkt werden bijna uitsluitend door de 'technische gemeenschap' (ICANN, IGF, WSIS, etc.) gemaakt. Overheden eisen echter een steeds prominentere rol op nu het belang van het internet op het gebied van economie en veiligheid groeit. Dit zien we in debatten over auteursrechten,

¹²⁶ TNO-rapport R10006, "Stimulerende en remmende factoren Privacy by Design in Nederland" (2012).

¹²⁷ www.digitaleoverheid.nl/onderwerpen/stelselinformatiepunt/stelsel-van-basisregistraties

terrorisme, veiligheid en online gokken.¹²⁸ Er zijn ook landen die 'hun deel' van het internet willen afschermen en in de toekomst zullen steeds meer landen technische capaciteiten krijgen. Wat D66 betreft moeten censuur, blokkades en persbreidel te allen tijde worden voorkomen.

In het belang van internetvrijheid is een diplomatieke benadering van internetgovernance nodig. Als eerste stap wil D66 een bindende internationale norm waarin centrale protocollen van het internet beschouwd worden als een neutrale zone, die overheden niet mogen betreden of verstoren. Grensoverschrijdende vraagstukken vragen immers om internationale afspraken. Zoals er verdragen zijn gesloten omtrent het gebruik van de zee, moet dit ook voor het internet gebeuren. Een verbod op misbruik van de kernprotocollen van het internet is in het belang van alle staten en bedrijven. Het vertrouwen van gebruikers in de talloze diensten die online worden aangeboden, variërend van internetbankieren tot chatten, is er immers van afhankelijk. Nederland kan gidsland worden door bij eigen wetgeving, beleid en operationele activiteiten de bescherming van de publieke kern van het internet voorop te stellen. Daarom wil D66 in de wet opnemen dat nieuwe wetgeving niet mag ingrijpen in een aantal centrale protocollen die het internet in goede banen leiden. Zo kunnen staten die in de toekomst een grotere rol gaan vervullen in het internetdomein overtuigd worden om het internet als mondiaal publiek goed in ere te houden. Niet alleen staten, maar ook grote technologiebedrijven en ngo's moeten hierbij betrokken worden.

Box14: Internetwaarden die Nederland internationaal moet uitdragen

- Een open en vrij internet
- Bescherming van het internet als publiek goed
- Recht op een zorgvuldige omgang met persoonsgegevens
- Recht op sterke versleuteling van data
- Maak het internet veiliger in plaats van kwetsbaarheden in software te misbruiken
- Goede bescherming van hackers en onderzoekers

128 Zo stelt het kabinet voor om in de kansspelwet een zogenaamde IP/DNS-blokkade op te nemen waardoor bepaalde gokwebsites vanaf een Nederlands IP-adres niet meer benaderd zouden mogen worden. D66 is hiertegen en wil dit uit de wet halen: <http://www.rtlnieuws.nl/economie/home/tweede-kamer-wil-ip-blokkade-invoeren-om-goksites-te-bestrijden>.

Hoofdstuk 4

Digitale veiligheid

Steeds meer vertrouwen we op het internet. Zo heeft de helft van de Nederlanders een mobiele app om zijn bankzaken te regelen¹²⁹ en gebruikt vrijwel iedereen Whatsapp voor communicatie met vrienden, familie en collega's.¹³⁰ We rekenen erop dat diensten veilig zijn. Maar wat verstaan we daar eigenlijk onder? Een veelgebruikt model is de “BIV-Driehoek” (of CIA-triad¹³¹). De drie letters staan voor: Beschikbaarheid: bij jouw informatie kunnen wanneer dat nodig is; Integriteit: de foutloosheid van jouw informatie; Vertrouwelijkheid: wie toegang heeft tot jouw informatie (en wie niet). In de dagelijkse praktijk: jouw internetbankieren ligt er niet uit als je het nodig hebt, jouw informatie blijft onveranderd in jouw cloud-opslag en jouw Facebook-account moet alleen jou toegang geven.

Steeds meer apparaten zijn verbonden met het internet. Een trend die door lijkt te zetten onder de noemer “Internet of Things”. Onderzoeksbureau Gartner gaat uit van een groei van krap vier miljard verbonden apparaten in 2014 naar 25 miljard in 2020.¹³² Niet alleen “traditionele” computers maar ook steeds meer apparatuur en gebruiksvoorwerpen. Je auto is verbonden met het internet voor navigatie, muziek en onderhoud; je koelkast geeft door dat de melk bijna over datum is en je kunt op afstand je lichten aan en uit zetten.

Nu het internet omvangrijker en intensiever wordt groeit ook de uitdaging om het veilig te houden. Dat ook auto's niet meer veilig zijn bewezen twee hackers in de Verenigde Staten door aan te tonen dat meerdere typen auto's te hacken zijn.¹³³ Op afstand namen zij de controle van het voertuig over en konden de rem en koppeling bedienen. Russische hackers zijn er in geslaagd geldmachines zo te hacken dat ze zonder pinpas geld uitspuugden.¹³⁴ De schade van cybercrime wordt op dit moment voor Nederland op zo'n 8 miljard geschat en zal – zeker als we niks doen – alleen maar stijgen.¹³⁵ De consequenties van een onveilig internet worden alleen maar ernstiger. Het zijn niet alleen maar onze social media accounts of e-mails die gehackt kunnen worden. Ons dagelijks leven kan in gevaar komen als stoplichten, sluizen of andere verkeerssystemen via het internet beïnvloed worden.

129 <http://www.slideshare.net/INGNL/samenvatting-resultaten-onderzoek-naar-gebruik-apps-mobiel-bankieren-onder-nlrs>

130 <http://tweakers.net/nieuws/94678/whatsapp-heeft-9-komma-5-miljoen-actieve-gebruikers-in-nederland.html>

131 <http://www.techrepublic.com/blog/it-security/the-cia-triad/>

132 <http://www.gartner.com/newsroom/id/2905717>

133 <http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>

134 <http://www.volkskrant.nl/tech/crimineel-zit-diep-in-onze-data~a4119347/>

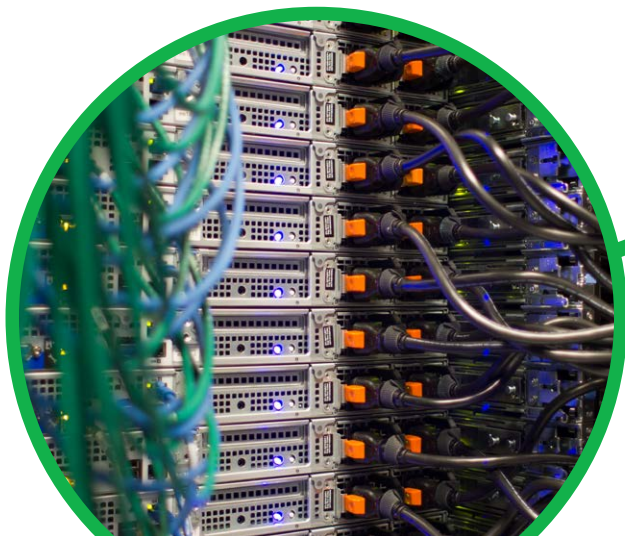
135 <http://www.volkskrant.nl/recensies/-cybercrime-kost-nederland-jaarlijks-8-miljard~a3669671/>

Tegelijkertijd gebeurt veel om het internet steeds veiliger te maken. Nieuwe technieken en meer aandacht voor veiligheid, ook in eerdere fasen van ontwikkeling van een systeem (“security by design”) zorgen ervoor dat wij het internet meestal probleemloos kunnen gebruiken. Daarbij levert digitalisering niet alleen maar bedreigingen op. Het internet zorgt voor meer dialoog en waar mensen praten wordt minder gevochten. De economische kansen die het internet biedt, juist voor mensen in achtergestelde delen van de wereld, zorgt voor welvaart en daarmee meer veiligheid. Daarnaast dragen ontwikkelingen die het internet gebruiken bij aan veiligheid. Zo wordt er minder met contant geld afgerekend, wat de kans en impact van winkeldiefstallen vermindert, en vormen drones, mits goed gereguleerd, een waardevolle bijdrage voor de politie en het leger.

Visie 2030: Nederland als Veilige haven en toevluchtsoord

Nederland heeft zijn digitale veiligheid op orde. Cybercriminaliteit is niet uitgebannen: we zijn nuchter en weten dat fouten kunnen voorkomen. Maar we proberen het zoveel mogelijk te voorkomen (preventie). Waar dat niet lukt ontdekken we fouten snel (detectie) en handelen we om de gevolgen te beperken (respons). Net als in de fysieke wereld werkt de overheid -in nauwe samenwerking met het bedrijfsleven- aan een veilige virtuele samenleving en is een betrouwbare partner voor burger en bedrijf. Internet is net als het wegen- of waternet een vanzelfsprekend onderdeel van de vitale infrastructuur.

Burgers zijn digi-vaardig en weten waar ze op moeten letten om het internet veilig te gebruiken. Het bedrijfsleven investeert in goede beveiliging van klantdata en bedrijfsgeheimen, met positieve gevolgen voor het vestigingsklimaat van Nederland. Ook ethische hackers en onderzoekers voelen zich dankzij duidelijke rechtsbescherming veilig in ons land. Omdat een veilig internet niet stopt bij de landsgrenzen werkt Nederland actief samen met andere landen en organisaties aan een veiliger internet voor iedereen. De overheid ondersteunt de ontwikkeling van veilige technieken, deelt en dicht -en maakt dus geen misbruik van- lekken en stimuleert de aanpak van cybercriminelen. Ook is er bij bedrijven meer aandacht voor veilige software doordat software voortaan onder de garantie van een product valt.



Aanbevelingen

Nu we steeds meer vertrouwen op het internet, moeten we zorgen dat we daadwerkelijk kunnen vertrouwen op het internet. Daarom doet D66 de volgende voorstellen:

Aansprakelijkheid voor nalatigheid door slechte software

Nu we meer op digitale diensten vertrouwen, vertrouwen we ook op de juiste werking van de software hierachter. Denk aan de software in je auto of de systemen die jouw gegevens bewaren bij je favoriete webwinkel. Fouten hierin kunnen leiden tot grote problemen. Dit kan door misbruik van het systeem door een derde of door foutieve werking van het systeem zelf. De uitdaging is dat software steeds complexer wordt. Veel softwaresystemen tellen miljoenen regels code en bijna wekelijks verschijnt voor veelgebruikte applicaties een update die de code vernieuwt. Dat laatste is noodzakelijk om fouten die ontdekt zijn te kunnen dichten. Niet genoeg aandacht aan de kwaliteit van je software besteden is een vorm van nalatigheid. Net zoals het nalatig is om niet over de brandveiligheid van producten na te denken. Ook het niet tijdig updaten van software onder jouw beheer is een vorm van nalatigheid. Zo ontstaat immers een risico op fouten.

Steeds meer bedrijven zijn softwareontwikkelaar¹³⁶ en moeten zich bewust zijn van de verantwoordelijkheid die hoort bij het leveren van software. Met het Internet of Things groeit dan ook het belang van duidelijke aansprakelijkheid voor softwaresystemen. D66 stelt voor dat consumentenbeschermingsregels, zoals garantie, ook van toepassing zijn op software. Zo weten organisaties dat zij met het aanbieden van een nieuwe dienst of product ook de verantwoordelijkheid aangaan deze deugdelijk te houden.

Bescherm onderzoekers en hackers

In het opsporen van kwetsbaarheden in software spelen goedwillige hackers een grote rol. Dit zijn vrijwilligers die systemen onderzoeken op kwetsbaarheden en deze melden aan de eigenaren zodat deze opgelost kunnen worden. Pas daarna wordt het lek openbaar gemaakt. Dit noemen we “Responsible Disclosure”. Steeds meer bedrijven zien de belangrijke rol van hackers in hun cyber-veiligheid. Ze starten programma’s op waarbij hackers geldbedragen krijgen voor het vinden van lekken. Dit begint een markt op zichzelf te worden. HackerOne is een Nederlandse Startup die een marktplaats vormt waar Hackers en bedrijven elkaar kunnen vinden. Google heeft in 2014 al meer dan \$ 1,5 miljoen uitgereikt aan Hackers in hun Security Reward Program.¹³⁷

Maar niet altijd worden goedwillige hackers warm verwelkomd. Soms omdat het

¹³⁶ Autofabrikanten, speelgoedmakers, producenten van huishoudelijke apparaten, ontwikkelaars van zorg- en onderwijssystemen, enzovoorts.

¹³⁷ <http://googleonlinesecurity.blogspot.com/2015/01/security-reward-programs-year-in-review.html>

aantonen van het lek betekent dat je het lek moet gebruiken. Je treedt het systeem van de ander binnen en vaak moet je ook bewijsmateriaal verzamelen, wat neerkomt op informatie (lees: persoonsgegevens) kopiëren. Daarmee betreden hackers een grijs juridisch gebied¹³⁸ en kiezen bedrijven voor vervolging van goedbedoelende personen. Voorbeelden zijn uitgevers waar je al hun boeken gratis kunt downloaden¹³⁹ of onderzoekers die de chip in de elektronische sleutels van Volkswagen kraken en door de rechter een verbod krijgen erover te publiceren.¹⁴⁰ Problematischer is de reactie van sommige bedrijven die geen goed gevolg geven aan de melding en het probleem niet oplossen.

De Nederlandse overheid heeft sinds 2013 een leidraad voor Responsible Disclosure. Deze leidraad verbiedt een aantal zaken als onderdeel van “ethisch hacken”, waaronder Brute Force aanvallen en Social Engineering. De leidraad werkt goed en daarbovenop heeft de rechtbank hackers meermalen zelfs ruimere rechten toegekend in het aantonen van misstanden.¹⁴¹ D66 wil dat hackers de juridische bescherming krijgen die past bij hun rol en vindt dat hackers die de leidraad hebben nageleefd nooit vervolgd worden. Internationaal moet Nederland een voortrekkersrol spelen in het goed behandelen van hackers. Binnen Europa door te pleiten voor meer uniforme regelgeving. Buiten de EU door als veilige haven voor hackers te fungeren. Hackers die vanuit Nederland hacken en de leidraad volgen worden niet vervolgd of uitgeleverd.

Kwetsbaarheden in software dichten en niet misbruiken

Niet alleen criminelen maar ook landen gebruiken kwetsbaarheden in software bij onderlinge cyber-oorlogsvoering. Zo werd het Stuxnet-virus (2010) gemaakt om Iran's nucleaire programma te saboteren.¹⁴² Stuxnet gebruikte “Zero-Day Exploits¹⁴³” om systemen binnen te dringen. Een ander voorbeeld is Hacking Team: een bedrijf uit Italië dat software ontwikkelt waarmee telefoons en andere apparaten gehackt kunnen worden. Deze software wordt waarschijnlijk gebruikt door overheden met minder goede bedoelingen,¹⁴⁴ maar als het aan het kabinet ligt mogelijk ook de Nederlandse politie. Als een kwetsbaarheid eenmaal bekend is, kan hij gedicht worden en verliest hij zijn waarde. Het ontdekken en verhandelen van deze Zero-Days begint een markt op zichzelf te worden. Steeds meer overheden realiseren zich dat ze de keuze hebben om deze lekken voor zichzelf te houden voor eigen gebruik of om ze te openbaren.

138 Meer hierover op de website en het boek “Helpende Hackers” van Chris van 't Hof. Zie: <http://cvth.nl/vo.htm>.

139 <http://www.cvth.nl/vo8.pdf>

140 <http://www.cvth.nl/vo6.pdf>

141 <http://computerworld.nl/beveiliging/84863-ethisch-hacker-mag-malware-plaatsen-van-rechter>

142 <https://vimeo.com/25118844>

143 Een “Zero-Day” is een kwetsbaarheid in software die onbekend is bij de maker ervan en het grote publiek, en daardoor gebruikt kan worden om software of een computersysteem binnen te dringen.

144 <http://www.automatiseringgids.nl/nieuws/2015/33/criminelen-gebruiken-tools-van-hacking-team-volop>

Documenten laten zien dat Amerikaanse geheime diensten beleid hebben ontwikkeld om deze keuzes te sturen.¹⁴⁵

Er is een probleem bij het bewaren van Zero-Days. De kwetsbaarheid die jij zelf kent (het geheime deurtje) kan ook bekend zijn bij anderen. Door de Zero-Day niet te publiceren, houd je het internet dus onveilig voor iedereen. D66 stelt daarom voor dat de Nederlandse overheid een non-proliferatie beleid voert op het vlak van Zero-Days. Dus geen Zero-Days achterhouden voor eigen gebruik maar ze actief publiceren om het internet veiliger te maken. En dit uitdragen in Europa en richting internationale partners. De Amerikaanse FBI bewandelde dan ook de verkeerde weg door de iPhone van een terreurverdachten zelf te kraken zonder de daarbij gebruikte kwetsbaarheid aan Apple te vertellen.¹⁴⁶ Net zoals wij geen wapens leveren aan landen waarvan we vermoeden dat mensenrechten er niet worden gerespecteerd, moeten we ook geen cyber-wapens leveren aan landen waar mensenrechten niet worden gerespecteerd. Naast een bijdrage aan een veiliger internet draagt dit ook bij aan het zijn van een veilige digitale haven en dus ons (digitale) vestigingsklimaat. Nederland kan zich wereldwijd profileren en zowel diplomatiek als economisch resultaat boeken.

Veilig gebruik van drones, geen gebruik killerrobots

Het civiele gebruik van drones biedt grote kansen, mits ze veilig – en zonder hinder – onderdeel uitmaken van het luchtruim. De inzet van drones biedt een enorm potentieel op een breed spectrum variërend van onder meer toepassingen in infrastructuur, precisielandbouw, media/journalistiek, noodhulp en transport en logistiek. Bovendien zorgt het commercieel gebruik van drones voor een belangrijke opkomende markt die economische groei, werkgelegenheid en innovatie kan stimuleren. Om dit potentieel volledig te kunnen benutten en het veilige en verantwoorde gebruik van drones te garanderen, zijn wel duidelijke (Europese) regels nodig, zonder grote verschillen tussen lidstaten.¹⁴⁷ Eenduidige en toekomstbestendige regels (over certificering, opleidingseisen, vlieghoogte, privacybescherming) voor drones van verschillende formaten zijn hierbij het belangrijkste. Ook moet voorkomen worden dat bepaalde drones op bepaalde plekken vliegen waar dat niet mag (nabij gebouwen, vliegvelden, kerncentrales), door middel van technologieën als ‘detect and avoid’ en *geofencing* kan dit voorkomen worden. Ook moeten alle drones geregistreerd worden door middel van een ID-chip. Zo kan de eigenaar van een drone te allen tijde achterhaald worden, hetgeen nodig is voor handhaving van de wettelijke aansprakelijkheid.

Het steeds terugkerende vraagstuk van aansprakelijkheid bij software en

145 <http://www.wired.com/2015/03/us-used-zero-day-exploits-policies/>

146 <http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?r=0>

147 Momenteel vallen alle drones onder het gewicht van 150 kilo nog onder de bevoegdheid van de lidstaten. Onder deze gewichtsklasse zijn de regels per land nogal verschillend.

geautomatiseerde handelingen, speelt zeker bij zogenaamde robotsoldaten of killerrobots. Landen als de VS, het Verenigd Koninkrijk, Frankrijk, Duitsland en Israël, maar ook China en Rusland, zijn bezig met de ontwikkeling hiervan. Wetenschappers en ondernemers als Stephen Hawking en Elon Musk hebben in een open brief opgeroepen tot een internationaal verbod voor een militaire mogendheid ze inzet en een nieuwe wapenwedloop losbarst. D66 ondersteunt dit pleidooi van harte.

Een sterker en onafhankelijker NCSC

De overheid beschikt over veel gevoelige informatie van burgers en voert processen uit waar heel Nederland vertrouwt. Het uitvallen van systemen bij bijvoorbeeld Rijkswaterstaat of datalekken bij Defensie kan grote impact hebben. De overheid doet veel om haar systemen digitaal veilig te houden. Met het instellen van een Rijks-CIO stroomlijnt zij de ICT voorzieningen: in 2001 waren er bijvoorbeeld 66 datacenters (elk ministerie had eigen centra en systemen). Dit is ondertussen teruggebracht tot vier die samenwerken, elkaar kunnen vervangen bij uitval en extra goed beveiligd zijn. En met het Nationaal Cyber Security Centrum (NCSC), het expertisecentrum voor cybersecurity, ontwikkelt de overheid haar cybersecurity-competenties.

D66 wil de rol van het NCSC verder versterken. Het NCSC moet een onafhankelijke organisatie worden zonder bemoeienis van de politiek, ministeries en andere instanties. Zoals het RIVM¹⁴⁸ (Rijksinstituut voor Volksgezondheid en Milieu) als kennisinstituut helpt om Nederland gezond te houden zou het NCSC kunnen helpen Nederland digitaal veilig te houden. Zo zorgen we dat het NCSC handelt vanuit kennis en expertise in plaats van politieke motieven. Advies op bijvoorbeeld het vlak van gebruik van VPN's of encryptie¹⁴⁹ zou het NCSC onafhankelijk moeten kunnen geven, zonder druk of invloed te voelen van andere overheidsinstanties als justitie of de AIVD. Daarnaast moet het NCSC ruimere bevoegdheden krijgen om een "digitaal veilige overheid" te borgen. Zo werken een aantal ministeries niet mee aan bepaalde beveiligingsmaatregelen van het NCSC.¹⁵⁰ Door samenwerking en een centrale aanpak verplicht te stellen kan de overheid haar cyber-beveiliging beter op orde brengen. Investeren in de slagkracht van het NCSC moet er ook toe leiden dat het NCSC meer kan openbaren over de ontwikkelingen op het vlak van cybersecurity en de trends die zij waarneemt.

Het NCSC speelt een belangrijke rol in het testen van de veiligheid van onze overheidssystemen. Door onderzoekers of *white hat hackers* los te laten op overheidssystemen testen zij de veiligheid van bestaande en nieuwe informatiesystemen. D66 is voor een systeem van beloningen voor het opsporen van kwetsbaarheden.

148 http://www.rivm.nl/RIVM/Missie_en_Strategie/Onafhankelijkheid

149 <https://www.ncsc.nl/actueel/nieuwsberichten/ncsc-publiceert-factsheet-wifi-onderweg-gebruik-een-vpn.html>

150 <http://www.volkskrant.nl/tech/crimineel-zit-diep-in-onze-data~a4119347/>

Werk samen met bedrijven op operationeel niveau

Een veilig internet is een gedeeld belang van overheid en bedrijfsleven. Beide hebben daarom baat bij het delen van informatie over het soort en de herkomst van cyberaanvallen, om van elkaar te leren en beter te anticiperen op cybercrime. Cybercrime is allang geen denkbeeldige dreiging meer. Sony werd in 2014 in grote verlegenheid gebracht toen een grote hoeveelheid informatie op straat kwam te liggen.¹⁵¹ En deze zomer hadden klanten van Ziggo tijdelijk geen internet doordat de DNS-servers een DDOS aanval ondergingen.¹⁵² Daarom investeren bedrijven in cybersecurity en daarbij geldt: meer weten over het type aanval maakt een betere verdediging mogelijk. Als de ene bank een aanval opmerkt uit een bepaald gebied kunnen andere banken zich hier op voorbereiden. Als de klanten van een webwinkel door social engineering worden belaagd kunnen andere webwinkels hun klanten waarschuwen voor soortgelijke aanvallen.

In de Verenigde Staten delen bedrijven binnen een sector informatie over cyberdreigingen via Information Sharing and Analysis Centers (ISAC's).¹⁵³ Ook Nederland kent deze overlegorganen. Zij krijgen informatie van het NCSC, delen op operationeel niveau informatie over cyberaanvallen,¹⁵⁴ verspreiden best-practices en werken in een vertrouwelijke setting. Tot nu toe beperkt deze aanpak zich tot vitale sectoren als water, energie, zorg, telecom en banken. D66 wil dat deze aanpak wordt uitgebreid naar alle economische sectoren die te maken hebben met cybercrime. Ook wil D66 dat bedrijven in hun jaarverslag een hoofdstuk over cybersecurity op te nemen zodat zij gestimuleerd worden na te denken over de online veiligheid van het bedrijf.

“Security by Design” en open source software als standaard

Te vaak blijkt achteraf dat het aansluiten van apparaten op internet of het eindeloos koppelen van databestanden tot onwenselijke en onveilige situaties kan leiden. Neem hackbare barbiepoppen of smart tandenborstels. Nadenken over de veiligheid van een apparaat of systeem moet beginnen bij het ontwerp en mag niet stoppen na de oplevering ervan. D66 stelt voor dat “*security by design*” een leidend principe wordt voor de overheid. Niet alleen in beleidsnota's maar ook in de praktijk.¹⁵⁵

Daarnaast wil D66 dat de overheid open source software als standaard neemt bij ICT-aanbestedingen in plaats te werken met het “Security through Obscurity”.¹⁵⁶ De gedachte achter dit (closed source) principe is dat je de betrouwbaarheid vergroot door de broncode geheim te houden. Echter, dit idee raakt achterhaald. Zelf kun je immers

151 <https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/>

152 <https://www.ziggo.com/nl/newsroom/persberichten/3997/ziggo-informeert-klanten-over-ernstige-aanvallen-op-ons-netwerk>

153 <http://www.dhs.gov/isao>

154 <https://www.ncsc.nl/samenwerking/publiek-private-samenwerking.html>

155 De motie van Elissen en Gesthuizen heeft dit als principe vastgelegd. Nu is het zaak dat dit doorleefd en nageleefd wordt.

156 https://nl.wikipedia.org/wiki/Security_through_obscurity

de fouten dan ook niet vinden en dichten. Daarom: open source als het kan, closed source als het moet. Bijkomend voordeel is dat andere overheden dan dezelfde (open) software kunnen hergebruiken. Indien closed source software onvermijdelijk is (zoals bij de ontwikkeling van defensiesystemen), moet dit gepaard gaan met voldoende software-audits om de veiligheid te garanderen, bijvoorbeeld via zogenaamde “zwakke schakel analyses”.

Een veilige infrastructuur in private handen

De overheid beheert het wegennet, de spoorwegen, het waternet en het elektriciteitsnetwerk via Rijkswaterstaat, ProRail en TenneT.¹⁵⁷ De infrastructuur van het internet is een systeem van private netwerken die op elkaar aangesloten zijn en als het ware samenkomen bij internet exchanges, zoals AMS-IX. Een van de grootste knooppunten ter wereld¹⁵⁸ en een cruciaal stuk van de infrastructuur. De vele vertakkingen van de netwerken vormen een ingebouwd veiligheidssysteem: als een knooppunt uitvalt kan dit vaak overgenomen worden door andere. Anders dan bij andere vitale infrastructuur ligt het beheer en de exploitatie van het internet bij de markt (hoofdzakelijk KPN en Ziggo). D66 ziet vooralsnog geen reden hier verandering in te brengen door de internet en telecominfrastructuur (gedeeltelijk) te nationaliseren door aandelen te verwerven. Dit zou ten koste gaan van de concurrentie waaraan de kwaliteit van het netwerk juist te danken is. Een buitenlandse overname van een telecombedrijf is echter niet ondenkbeeldig.¹⁵⁹ Dat neemt niet weg dat wettelijke verplichtingen en Nederlandse regels onverminderd moeten worden nageleefd. Ook zijn er voldoende mogelijkheden om de veiligheid van communicatie en vitale diensten in zo'n situatie te waarborgen.¹⁶⁰

Naast hardware is er veel software (en zijn er protocollen) nodig om het internet draaiende te houden. Een voorbeeld is encryptie: software waarmee wij onze verbindingen op het internet versleutelen zodat niemand anders mee kan lezen, zoals OpenSSL. Deze versleutelde verbindingen gebruiken we om te communiceren met onze bank, onze e-mail-provider, Facebook en nog veel meer. In april 2014 bleek dat er een lek in deze software zat. Dit werd bekend als de Heartbleed Bug.¹⁶¹ OpenSSL wordt ontwikkeld door welgeteld één fulltime medewerker en een handjevol vrijwilligers.¹⁶² D66 stelt daarom voor dat de overheid financieel bijdraagt aan de ontwikkeling van open-source software.

157 Rijkswaterstaat is onderdeel van het ministerie van I&M, ProRail en TenneT zijn beide staatsdeelnemingen.

158 <https://ams-ix.net/>

159 Dit bleek in 2013 toen America Movil KPN dreigde over te nemen.

160 Toen de overname van KPN door América Movil speelde heeft het kabinet een extra instrument boven de bestaande wetgeving geïntroduceerd: een verklaring van geen bezwaar voor het verwerven van zeggenschap over telecombedrijven, het doorverkopen van vitale infrastructuur en het benoemen van bestuurders. Ook aanvullende contractuele afspraken zijn mogelijk.

161 <http://heartbleed.com/>

162 http://www.huffingtonpost.com/2014/04/10/heartbleed-bug_n_5120457.html

Veilige Digitale Authenticatie en Identificatie

In de fysieke wereld identificeer je je met een paspoort of ID-kaart uitgegeven door de overheid. Bijvoorbeeld in contact met overheidsorganen (politie, gemeente, etc.) en bedrijven (banken, luchtvaartmaatschappijen). Online is de rol van de overheid bescheidener. Alleen in contact met de overheid (en zaken als een zorgverzekering) is er een publiek identificatiemiddel: DigiD.

Steeds vaker zijn private partijen actief in online identificatie. Een Facebook-account is steeds meer een universeel account waarmee je inlogt op andere diensten. Daarmee vertrouwen deze diensten dus op het oordeel van Facebook. De regering van Estland heeft een andere route gekozen. Het identificatiebewijs van de overheid heeft ook een digitale component en biedt de mogelijkheid om je online te identificeren door bijvoorbeeld e-mails digitaal te ondertekenen.¹⁶³ Daarmee is een universeel bruikbare en vertrouwde manier van online identificeren ontstaan. Dit maakt ook nieuwe diensten mogelijk zoals online medicijnrecepten, ov-betalingen en e-voting. Dat een nationaal systeem hiervoor geen sinecure is bewees Zuid-Korea. Hacks van credit card-bedrijven en fouten in het ID-systeem hebben dit onder druk gezet.¹⁶⁴

Overheid en bedrijfsleven werken samen aan de opvolger van DigiD: Idensys. Dit platform moet een uniforme identificatie en authenticatiedienst opleveren voor zowel publieke als private diensten met verschillende zekerheidsniveaus. D66 stelt drie voorwaarden aan systemen voor online identificatie en authenticatie. Ten eerste moet er altijd een publieke authenticatiedienst zijn om in te loggen op overheidsdiensten en deze mag niet significant ongebruiksvriendelijker zijn.¹⁶⁵ Ten tweede moet het mogelijk blijven om anoniem te internetten. Niet voor alle diensten waarbij je moet inloggen hoeft je ook gelijk alle (persoons)gegevens te hebben. Voor een bioscoopkaartje of een e-book kan een e-mailadres voldoende zijn. De gebruiker kan nu maar beperkt invloed uitoefenen op de gegevens die worden gevraagd. De standaard moet hier zijn: zo weinig mogelijk gegevens delen. Hoe je dit ook organiseert: het is cruciaal dat persoonsgegevens niet zomaar te herleiden zijn tot de persoon in kwestie. Ten derde moet het Idensys stelsel waarborgen dat niet meer informatie van de gebruiker wordt doorgegeven aan de online dienst dan strikt noodzakelijk. Een drankwinkel hoeft bijvoorbeeld niet te weten hoe oud je bent bij de aankoop, alleen maar dat je ouder dan 18 bent. Dit “attribuut” kan Idensys doorgeven in plaats van jouw leeftijd.

163 <https://e-estonia.com/component/electronic-id-card/>

164 <http://www.engadget.com/2014/10/14/south-korea-id-breach/>

165 Het Idensys stelsel maakt het mogelijk om in te loggen op overheidsdiensten via private authenticatiediensten (mits deze aan het betrouwbaarheidsniveau voldoen). Daarmee zou je bijvoorbeeld via de inlogdiensten van je bank op de website van de Belastingdienst kunnen inloggen.

Box15: Belangrijkste cyberdreigingen¹⁶⁶

- Cryptoware en ransomware: programma's die een computer (of gegevens die erop staan) blokkeren waarna geld geëist wordt om de computer weer te "bevrijden".
- Phishing: criminelen lokken gebruikers naar een "nep-website" (bijvoorbeeld je bank) om inloggegevens in te voeren en krijgen zo beschikking over de inloggegevens van derden.
- Social Engineering: criminelen doen zich voor als iemand anders (bijvoorbeeld een collega) en proberen via e-mail of telefoon wachtwoorden of gevoelige informatie te bemachtigen.
- DDOS: een "Distributed Denial of Service" aanval. Door met heel veel (vaak gehackte) computers tegelijkertijd verzoeken naar een computersysteem te sturen leg je het systeem plat. Zo kun je websites onbereikbaar maken.
- Man-in-the-Middle aanvallen: dit zijn aanvallen waarbij informatie tussen twee communicerende partijen onderschept wordt zonder dat beide partijen daar weet van hebben.
- Bruteforce: het kraken van een wachtwoord door "domweg" alle opties te proberen zoals bij een cijferslot. Zeker super- of kwantumcomputers kunnen in de toekomst snel wachtwoorden kraken.

Voer campagne vóór cyberhygiëne

Online is de gebruiker de zwakste schakel. Voor een veilig internet is digitaal bewustzijn cruciaal. Veel cybercriminaliteit is niet *high tech* maar *low tech* en gebaseerd op onoplettendheid of onwetendheid van gebruikers. Voorbeelden hiervan zijn phishing en social engineering.

De beste manier om infecties te voorkomen is je handen wassen. Om digitaal "schoon" te blijven is cyberhygiëne nodig. Denk hierbij aan praktische zaken als het geregeld wisselen van wachtwoord ("123456" is het meest gebruikte wachtwoord!), het niet downloaden van verdachte attachments en het geregeld installeren van updates.

¹⁶⁶ Volgens het Cybersecuritybeeld Nederland 2015 van het NCSC zijn cryptoware en phishing de grootste gevaren. Een ruime opsomming van alle mogelijke cybergevaren staat beschreven in het boek "Cybergevaar" van Eddy Willems (2013).



Bits of Freedom heeft een *Toolbox*¹⁶⁷ waarmee iedereen veiliger gebruik kan maken van het internet. Deze bevat tips voor software (antivirus, browser) en het gebruik ervan (altijd updaten, veilige instellingen). Het Centrum voor Informatiebeveiliging en Privacybescherming¹⁶⁸ ontwikkelt informatieproducten voor burgers, bedrijven en overheid. D66 wil extra investeren in cyberhygiëne via publiekscampagnes en onderwijs. Zoals rijden onder invloed met “Bob jij of Bob ik” een pakkende slogan heeft gekregen is het nu zaak slechte wachtwoorden en onbeschermd gebruik van open wifi uit te bannen. Ook identiteitsfraude verdient meer aandacht.¹⁶⁹ En voor kinderen worden digitale vaardigheden steeds belangrijker. In het onderwijs dient dit een vaste component te worden.

Als bewaarders van persoonlijke en gevoelige informatie van burgers hebben overheidsmedewerkers een grote verantwoordelijkheid. De overheid kan zich geen grote blunders veroorloven en investeringen in veilige systemen zijn zinloos zonder doelgerichte training van medewerkers – van gamification tot het nabootsen van social engineering. Het Nationaal Cyber Security Centrum (NCSC) is hierbij een belangrijke bron van kennis.

167 <https://toolbox.bof.nl/>

168 <http://www.cip-overheid.nl/>

169 Wie denkt dat dit alleen bij anderen voorkomt, moet het boek “Komt een vrouw bij de H@cker” van Maria Genova (2014) eens lezen.

Financieel Overzicht

- | | |
|---|---------------|
| • Investeren in onderzoek en innovatie | €1 Miljard |
| • Versterken positie Autoriteit Persoonsgegevens | € 17 miljoen |
| • Versterken positie Autoriteit Consument & Markt | € 6 miljoen |
| • Versterken positie CTIVD | |
| • Inclusief uitbreiding naar toezicht op opsporingsdiensten | € 4 miljoen |
| • Onafhankelijk maken NCSC | € 5 miljoen |
| • Betere campagne cyberhygiëne | € 0,5 miljoen |

Verantwoording en geraadpleegde bronnen

Met deze technologievisie wil D66 een bijdrage leveren aan het steeds intensievere en belangrijkere debat over de impact van internet, digitale technologie en data op onze samenleving. Voor de samenhang van dit verhaal hebben we de vele deelonderwerpen verdeeld over vier grote hoofdthema's: **vrijheid, veiligheid, economie en het publieke domein**. Omdat deze alle vier onlosmakelijk onderdeel van het debat zijn en elkaar ook voortdurend raken, hebben we hier geen hiërarchie in aangebracht. Als politieke partij richten we ons in deze visie hoofdzakelijk op de rol van de overheid in het digitale domein. Dat de overheid een cruciale rol te vervullen heeft, neemt niet weg dat burgers en bedrijven ook veel zelf kunnen doen om hun positie te versterken en kansen te benutten.

Deze technologievisie is tot stand gekomen onder verantwoordelijkheid van de Tweede Kamerfractie van D66. Bij het ontwikkelen ervan hebben we gebruik gemaakt van een grote groep externe deskundigen. In het voorjaar van 2015 hebben we vier rondetafelgesprekken (over vrijheid, veiligheid, economie en het publieke domein) georganiseerd en in de zomer van dat jaar hebben we circa 20 individuele zomergesprekken gevoerd. Deze betrokkenen konden tevens input leveren op een eerste versie. Iedereen kon reageren via de speciale projectwebsite <https://internet.ideeend66.nl>.

De volgende personen hebben langs deze wegen een waardevolle bijdrage geleverd:

Erwin Anrad Gaur (Platform Makers)

Christiaan Alberdink Thijm (Bureau Brandeis)

Joost Bazelmans (Bomberbot)

Arie van Bellen (ECP)

Erwin Bleumink (SURFNET)

Koos de Boer (Codeuur)

Lieke Boon (VHTO)

Xander Bouwman (D66)

Heleen Bouwmans (Het ABC)

Annelien Bredenoord (D66, Eerste Kamerlid)

Paul Breitbarth (Autoriteit Persoonsgegevens)

Dennis Broeders (Wetenschappelijke Raad voor het Regeringsbeleid)

Lotte De Bruijn (Nederland ICT)

Peter de Bruijn (Studio Veiligheid)

Frits Bussenmaker (CIONET)

Marieke Dekker (Liberty Global)

Nico van Eijk (Universiteit van Amsterdam)

Thomas Myrup Kristensen (Facebook Europa)

Sietske Faling (D66)

Pim van der Feltz (Google)
Bastiaan Goslings (AMS-IX)
Stijn Grove (Dutch Datacenter Association)
Wim Hafkamp (Rabobank)
Jos Huigen (KPN)
Lennart Huizing (Stichting Open Source & Overheid)
Martijn Hos (Thuiswinkel.org)
Chris van 't Hof (zelfstandig onderzoeker/schrijver)
Tom van der Horst (D66)
Robbert van den Hoogen (Stichting Praktijkleren)
Auke van Hout (Adatus)
Maarten Hillenaar (voormalig CIO Rijk)
Bart Jacobs (Radboud Universiteit)
Peter Jacobs (ING)
Pieke Jansen (Incentro)
Jacob Kohnstamm (Autoriteit Persoonsgegevens)
Ilse Koning (SURFNET)
Floris Kreiken (Bits of Freedom)
Koert Krouwel (It's Value)
Rogier Klimbie (Google)
Oscar Kneppers (Rockstart)
Tom Kunzler (Open State Foundation)
Arie Landsmeer (Ziggo)
Bart van der Linden (Nyenrode)
Laura van der Lubbe (Edutechno)
Danny Mekic (publicist, internetdeskundige)
Frank van Mil (Hans van Mierlo Stichting)
Alf Moens (SURF)
Geert Munnichs (Rathenau Instituut)
David de Nood (VNO-NCW)
Jos van Nunen ((Lumens Groep)
Frank van Oirschot (ExMachina Group)
Vincent Oord (D66)
Jurriaan Propper (Adstrat)
Frans van der Reep (KPN)
Pieter Rogaar (D66)
Daniel Ropers (Bol.com)
Marietje Schaake (D66, Europarlementariër)
Maarten Simon (SIDN)
Janneke Sloetjes (Netflix)
Ton Siedsma (Bits of Freedom)

Jeroen Slobbe (D66)
Michiel Steltman (Stichting Digitale Infrastructuur Nederland)
Floor Terra (D66)
Boris Veldhuijzen van Zanten (The Next Web)
Evert Jan Verbeij (D66)
Stas Verberkt (D66)
Gert Wabeke (KPN)
Bas Wallage (D66)
Brenno de Winter (zelfstandig journalist)
Renee Witsenburg (Informatica docent Hyperion Lyceum)
Elise van Zeeland (D66)
Rejo Zenger (Bits of Freedom)
Carsten Zwaaneveld (D66)

Naast alle in de voetnoten genoemde bronnen hebben wij veel gehad aan de volgende publicaties:

Cybersecuritybeeld Nederland (CSBN-4), Nationaal Cyber Security Centrum (2014)
Cybersecurity and Cyberwarfare, P.W. Singer and Allan Friedman (2014)
Databases, Rathenau Instituut (2010)
De Ondernemende Staat, Mariana Mazzucato (2014)
De Publieke kern van het internet, WRR (2015)
De Rationele Optimist, Matt Ridley (2010)
De Rechtstaat in Cyberspace (Inaugurele Rede), Mireille Hildebrandt (2011)
De Revolutie van Big Data, Anwar Osseyran & Willem Vermeend (2014)
De Robot de baas, WRR (2015)
Helpende Hackers, Chris van 't Hof (2015)
ICT, kennis en economie 2015, Ministerie van Economische Zaken en Centraal Bureau voor de Statistiek (2015)
Internet of Things, Willem Vermeend & Jan Willem Timmer (2016)
Internet is not the answer, Andrew Keen (2014)
Onder de motorkap van het Internet, Bits of Freedom (2013)
Klaar voor de Toekomst? Adviesraad voor Wetenschap, technologie en innovatie (2015)
Werken aan de Robotsamenleving, Rathenau Instituut (2015)

Het schrijfteam,

Kees Verhoeven (Tweede Kamerlid D66)
Marijn van Vliet (beleidsmedewerker D66-fractie)
Myrthe van Dieijen (Route66)
Dick van Egmond (Route66)
Nick Mastenbroek (Route66)
Ouke Arts (Route66)
Jan van der Voet (stagiair D66-fractie)

