



MEER DAN ENEN EN NULLEN

DIGITALISERINGSVISIE

APRIL 2023

Christen
Unie

Colofon

Meer dan enen en nullen. Digitaliseringsvisie ChristenUnie

Amersfoort, april 2023

De digitaliseringsvisie is ontwikkeld in opdracht van het Landelijk Bestuur van de ChristenUnie, naar aanleiding van Motie Digitaliseringsvisie, die werd ingediend op het 43e partijcongres van de ChristenUnie (2021).

Werkgroep

Michel Klein (voorzitter)
Elsbeth van den Hazel
Maaïke Harmsen
Mirjam Kosten (WI)
Rolf Hoving
Wouter Teeuw

Uitgave

ChristenUnie

 Geef geloof een stem



Fotografie

Coverbeeld Succulent Frenzy Edgar Castrejon via Unsplash

Vormgeving

Carola van der Krieke
Wouter Muskee
Aart Deddens (tekstredactie)

Met dank aan allen die in gesprekken of als meelezer hebben meegedacht bij het ontwikkelen van deze visie.

‘MEER DAN ENEN EN NULLEN’

Digitaliseringsvisie

April 2023

Inhoud

Hoofdstuk 1. Inleiding	6
Hoofdstuk 2. Waarden vanuit de beginselverklaring	11
2.1. Uitgangspunten voor overheidshandelen in digitaliseringsvraagstukken	12
2.2. Menselijke waarden in digitale tijden	14
2.3. Samenlevingsdoelen in tijden van digitalisering	16
Hoofdstuk 3. Afwegingen en richtlijnen	18
3.1. Gepersonaliseerde advertenties	18
3.2. Toegankelijkheid digitale wereld (en recht op niet-deelname)	19
3.3. Ruimte bieden aan publiek debat	21
3.4. Polarisatie en veiligheid	23
3.5. Cryptocurrency	24
3.6. Online onderwijs	25
3.7. Algoritmische besluitvorming	25
3.8. Autonome wapensystemen	27
3.9. Digitale identificatieplicht	28
3.10. Digitaal paspoort of e-identity	30
3.11. Regulering van datagebruik	31
3.12. Bewaren en vernietigen van gegevens (datajubeljaar)	33
3.13. Consequenties van digitalisering voor veiligheid	35
3.14. Omgaan met sociale media	36
3.15. Leefbare kernen	38
Hoofdstuk 4. Politieke speerpunten	39
Bijlage – Waar gaat het over?	42
Hooggespannen verwachtingen	42
Wat is er eigenlijk nieuw?	42
Internet: surface, deep en dark web	42
Algoritme	43
Vooroordelen en discriminatie door algoritmen	41
Sociale media	45
Blockchain en cryptocurrency	45
Digitale identiteit	46
Cybersecurity	47
Privacy	47
Algemene verordening gegevensbescherming (AVG)	47
Bibliografie	49

Voorwoord

Voor u ligt de digitaliseringsvisie van de ChristenUniewerkgroep Digitalisering. De ontwikkeling van deze visie volgt uit de wens van de leden van de ChristenUnie om een eigen visie op digitalisering te formuleren die ChristenUniewaarden als uitgangspunt neemt en die bruikbaar is in de politieke praktijk.¹ Het hoofddoel van deze visie is dan ook om ChristenUniepolitici een leidraad te geven bij het maken van politieke afwegingen met betrekking tot digitaliseringsvraagstukken.

Digitalisering speelt een steeds belangrijker rol in de samenleving: de ontwikkelingen raken aan de inrichting van de samenleving en de manier waarop we samenleven. In al die veranderingen onderscheidt de ChristenUnie als christelijk-sociale partij blijvende waarden en uitgangspunten. Zij vormen ijkpunten voor een consistent ChristenUniegeluid in een steeds veranderend digitaliseringslandschap.

Werkwijze

Voor de ontwikkeling van deze visie heeft de werkgroep gesproken met experts in en buiten de ChristenUnie op het gebied van digitalisering, in verschillende al dan niet virtuele gespreksrondes. Ook hebben de leden van de ChristenUnie op verschillende momenten de gelegenheid gekregen zich uit te spreken over onderdelen van deze visie. Als we in het vervolg van deze visie in de eerste persoon meervoud spreken, dan sluiten 'we' als werkgroep dus onze leden van de ChristenUnie in, met wie zoveel mogelijk is afgestemd.

Opzet

In het eerste hoofdstuk lichten we toe met wat we met digitalisering in het algemeen bedoelen. Daarna bespreken we op welke manier digitale technologie en digitalisering vanuit onze ChristenUnietraditie gewaardeerd kunnen worden en welke grondhouding ten opzichte van digitale technologie past bij onze politieke uitgangspunten. Het tweede hoofdstuk bevat waarden en uitgangspunten uit de ChristenUnie die een rol kunnen spelen in de beoordeling van digitaliseringsvraagstukken. Het derde hoofdstuk schetst een aantal casussen die langs de meetlat van de uitgangspunten en waarden van hoofdstuk twee gelegd worden. In een kort vierde hoofdstuk sluiten we af met een aantal politieke aanbevelingen. In een bijlage komen de belangrijkste begrippen en aspecten van digitalisering aan bod. Deze bijlage is vooral bedoeld voor mensen die een introductie in het thema goed kunnen gebruiken.

Het doel van deze visie is niet om een definitief oordeel over digitaliseringsvraagstukken te vellen. Liever nodigen we ChristenUniepolitici uit om vanuit deze benadering van technologie naar een voorliggend vraagstuk te kijken en de uitgangspunten en waarden te wegen in het maken van politieke keuzes.

¹ Motie 'Digitaliseringsvisie', ingediend op het 43e partijcongres van de ChristenUnie (2021).

Hoofdstuk 1. Inleiding

Wat bedoelen we met digitalisering?

Het ongevraagde advies van de Raad van State over digitalisering (2018) geeft goed weer dat digitalisering meer is dan geschreven informatie digitaal opslaan: 'In de meest basale omschrijving van het begrip digitalisering gaat het alleen om de omzetting van gegevens (opgebouwd uit letters, cijfers en beelden) in digitale vorm, dus in nullen en enen (binair). In het dagelijks spraakgebruik bedoelen we er veel meer mee: een groot aantal technologieën, zoals algoritmen, big data, digitale platformen, kunstmatige intelligentie, robotica, biometrie, persuasieve technologie, augmented reality [...] en virtual reality. Digitalisering betreft ook niet alleen het verzamelen en uitwisselen van gegevens, hoewel informatieproducten een belangrijke rol spelen. Het gaat veel breder om het vervangen van bestaande middelen, methoden en organisatievormen door nieuwe digitale werkwijzen, met vaak grote gevolgen.'² Voor deze publicatie definiëren wij digitalisering daarom breed als: het proces waarin digitale informatie, communicatienetwerken en geautomatiseerde besluitvorming een steeds grotere rol gaan spelen in de maatschappij.

De christelijke denktraditie: wereldbeeld, mensbeeld en de plaats van politiek

De ChristenUnie is een partij die gefundeerd is op haar grondslag: 'Gedreven door Gods liefde en Christus' koningschap wil de ChristenUnie zich inzetten voor de samenleving en het bestuur van ons land. Zij erkent dat de overheid door God is gegeven en in Zijn dienst staat, geroepen is om recht te doen en vrijheid en vrede te beschermen, wereldwijd. De ChristenUnie baseert haar politieke principes op de Bijbel, Gods gezaghebbende en door Hem geïnspireerde Woord.'³

Op basis van die grondslag zoeken wij vrede en recht, ook in bespreking en doordenking van digitaliseringsvraagstukken. De omgang met digitale technologieën wordt mede bepaald door hoe we kijken naar de wereld, naar mensen en naar politiek.

De wereld

Als christenen geloven we dat de wereld op dit moment niet volmaakt is en dat de technologische ontwikkelingen niet tot een perfecte wereld kunnen of zullen leiden. In onze dagelijkse politieke praktijk impliceert dit, dat wij er rekening mee houden dat ook onze digitale systemen niet volmaakt zullen zijn. Het betekent dat we digitalisering realistisch willen benaderen, met oog, niet alleen voor de mooie mogelijkheden van digitalisering, maar ook voor de negatieve effecten ervan. Ook het gebruik van digitale systemen door de overheid vindt plaats in die context van gebrokenheid en daarom moeten we rekenen op en rekening houden met kwetsbaarheden, met onbedoeld en bedoeld gebruik ten kwade.

Wij mensen

Wat we zeggen over de wereld waarin we leven, geldt ook voor mensen: we willen vaak het goede doen en falen daarin ook vaak. We weten niet altijd wat het goede is om te doen. We zijn als mensen vrij om te handelen en zijn verantwoordelijk voor ons handelen naar God, naar elkaar en onszelf. Als burger dragen we medeverantwoordelijkheid voor de samenleving. Politici hebben hierin een extra verantwoordelijkheid en zijn dienstbaar aan de samenleving. Dienstbare en verantwoordelijke politici zoeken ook in digitaliseringsvraagstukken naar publieke gerechtigheid: het gemeenschappelijk belang, de bescherming van kwetsbaren, het bestrijden van onrecht en het beschermen van recht.

² Raad van State, *Ongevraagd advies over de effecten van de digitalisering voor de rechtsstatelijke verhoudingen* (Den Haag: RvS, 2018) 3-4.

³ ChristenUnie, *Beginselverklaring: Vrede zoeken, recht doen* (Amersfoort: ChristenUnie, 2018) 2.

De politiek van hoop

Fantastische digitale technieken kunnen de indruk geven dat er voor elk menselijk probleem wel een technische oplossing is. Onze hoop zou dan gericht zijn op technologische oplossingen. Maar christelijke hoop begint bij het geloof dat God erbij is, dat Hij de Immanuel is, wat de toekomst ook zal brengen. God maakt uiteindelijk alles nieuw, wij kunnen die totale vernieuwing niet zelf realiseren (Openbaringen 21, 22). Het leven van een gelovige en een christen-politicus in het hier en nu is nadrukkelijk een leven van hoop op dat nieuwe begin. God blijkt hier en daar een begin van die vernieuwing nu al tot stand te brengen, als teken en voorproef van Zijn uiteindelijke redding. Hij schakelt ons daarbij in.

Het evenwicht van hoopvolle politiek in een gebroken wereld hebben we nodig in de omgang met digitaliseringsvraagstukken. In het denken over digitalisering betekenen deze uitgangspunten dat we digitalisering benaderen als een fenomeen waarbij we, net als bij andere vormen van techniek, vrijmoedig zoeken naar vormen van digitalisering die vrede en recht kunnen bevorderen. In vaak technische discussies over digitalisering blijven we dan ook op zoek naar de richting van een digitaliseringsvraagstuk, waarbij we dus niet alleen vragen 'hoe', maar ook 'waarom?' en 'waarheen?'.

Hoe benaderen we digitale technologie?

Binnen de ChristenUnie kunnen we putten uit een rijke traditie van technologiekritiek. We noemen in het bijzonder professor Egbert Schuurman, die van 1983 tot 2011 senator was voor de RPF en later voor de ChristenUnie. In talloze publicaties over techniek en onze benadering daarvan geeft Schuurman een gedegen analyse van de verschillende motieven – motieven die ook haaks kunnen staan op christelijke waarden. In het beheer van de schepping is het rentmeesterschap een belangrijk christelijk motief; de aarde is niet van ons; we hebben de opdracht om deze te bewerken en te bewaren.

Wij mensen kunnen dat doen door gebruik te maken van de menselijke hulpmiddelen van techniek en technologie in het algemeen. Technologie is echter niet neutraal, maar ontworpen door mensen met allerlei bedoelingen – goede en slechte – en vanuit diverse belangen. De ontwikkeling van technologie kan zowel gericht zijn op menselijke autonomie als op menselijke verbondenheid. Ze kan gericht zijn op maximale winst voor aandeelhouders of rekening houden met de meest kwetsbare groepen in de samenleving. Ze kan zowel gericht zijn op genot en consumentisme als op het behoud van natuur. Het zijn mensen die digitale technieken ontwerpen en paradoxaal genoeg geldt dat aan die abstracte technieken tegelijk niets menselijks vreemd is. Er zijn goede technieken waar we slecht gebruik van maken en er zijn ook slechte technologieën. Daarbij komt dat we niet losstaan van de technologieën die we maken en gebruiken. We zijn onderworpen aan de technologie die we zelf tot stand brengen: technologie kan ons denken en handelen veranderen en ons sturen, ten goede en ten kwade, bedacht en onbedacht.

De kritische analyses en waarschuwingen van Schuurman voor de transformerende invloed van het technicisme op ons denken en de maatschappij, nemen wij ter harte. Tegelijk blijven we niet bij kritiek, maar roepen we overheid en politiek op om, met deze kritiek in gedachten, andere wegen in te slaan in het gebruik van digitale technologie door overheid, bedrijven en de maatschappij.

We proberen vanuit deze denktraditie, die niet alleen de technologie maar ook haar motieven weegt, een weg te zoeken in onze omgang met digitalisering. De Amerikaanse software-ingenieur en hoogle-raar computerwetenschap Derek C. Schuurman, die niet alleen de achternaam maar ook het gedachtegoed met Egbert Schuurman deelt, biedt in zijn boek een inleiding in de omgang met digitalisering vanuit christelijk perspectief.⁴ Derek Schuurman onderscheidt vier manieren waarop we kunnen omgaan met digitalisering en computertechnologie: onverschilligheid, en respectievelijk het omarmen, afwijzen en cultiveren (ontwikkelen) van verantwoorde technologie.

In de praktijk benaderen we digitalisering en computertechnologie vaak minder principieel en kent onze omgang met techniek elementen van alle vier genoemde houdingen. Toch helpt de schets van deze

⁴ Derek Schuurman, *Shaping a Digital World. Faith, Culture and Computer technology* (Westmont: IVP Academic Publishing, 2013) 24.

uitersten om onze grondhouding ten opzichte van technologie scherp te krijgen en dat is van belang om als ChristenUnie tot een consequente politieke lijn te komen. We bespreken afwijzing, onverschilligheid en omarming als minder geschikte politieke lijnen. Vervolgens komen we uit bij cultivering als een zinvolle benadering van digitale technologie voor de ChristenUnie.

Afwijzing

Een afwijzende houding van (digitale) technologie kunnen we begrijpen vanuit de terechte bezorgdheid over de onontkoombare en overheersende rol die digitale technologieën in ons leven spelen. Gelovigen zullen echter niet zomaar principieel voor een totale afwijzing van techniek an sich zijn: zij zijn geroepen tot het bewerken en bewaren van de aarde en voor dat bewerken gebruiken we allerlei gereedschappen. Van landbouw tot muziek, van riolering tot wetenschapsbeoefening: de mens is ertoe geroepen, in samenwerking met anderen.

'Het teken van het beest'

Afwijzing van digitale technologie in christelijke kringen kan ook ontstaan door een interpretatie van Bijbelteksten over de naam van het beest of het getal van de naam op hun voorhoofd (Openbaring 13 vers 17), 'Alleen mensen met dat teken konden kopen of verkopen.' Al eeuwenlang zijn er, afhankelijk van tijd en plaats, concrete invullingen gegeven van dat teken. In de recente geschiedenis zijn bijvoorbeeld postcodes, streepjescodes, en QR-codes (al dan niet van het coronatoegangsbewijs), en digitale identiteitsbewijzen geïnterpreteerd als 'teken van het beest'. Deze interpretatie maakte dat sommige gelovigen niet te maken wilden hebben met ontwikkelingen als QR-codes. Nu zijn de meeste bijbelcommentaren het erover eens dat de apostel Johannes dit schreef in een tijd waarin de christenvervolgingen voor het eerst op grote schaal plaatsvonden. Johannes roept met zijn visioenen op om niet mee te doen aan de keizercultus en integendeel te volharden in tijden van vervolging. Voor christenen vandaag betekent deze tekst dat wij ons niet in mogen laten met de verering van 'keizers' – of die nu verschijnen in de vorm van macht, status of geld – maar ons vertrouwen op God moeten blijven stellen. Ook zonder dat we digitalisering an sich als duivelse macht duiden, kleven er genoeg problemen aan op het gebied van privacy, macht en inclusie, die we later in deze visie bespreken.

Onverschilligheid

Een tweede houding richting digitalisering kan zijn dat men er onverschillig tegenover staat en digitale techniek als iets neutraals ziet: het is immers maar een fysisch proces dat door mensen vormgegeven wordt. Egbert Schuurman heeft in zijn filosofie laten zien dat deze houding gevaarlijker is dan het afwijzen zelf, omdat zij blind is voor de ideologische kracht van technologisch denken. Technologie wordt ontworpen, vormgegeven en gebruikt door mensen. Onze technologie is daarmee te zien als een product van onze cultuur en niet als een waarde vrij domein.⁵

Omarmen

Een derde houding tegenover digitalisering is die van optimisme en omarming. Die houding zien we terug bij bedrijven, overheden en consumenten die onbezorgd de vruchten van digitalisering plukken, zonder oog te hebben voor of in aanraking te komen met schaduwkanten. Die houding van omarming is te begrijpen vanuit de onmiskenbare voordelen en mogelijkheden die digitalisering biedt. Digitalisering gaat samen met gemak, kostenreductie en efficiëntie. Overheden en bedrijven kunnen met digitale toepassingen hun burgers en klanten beter bereiken. Daarnaast kan omarming van digitalisering ook een meer fundamenteel karakter hebben, vanuit de gedachte dat technologie wel degelijk in staat is om grote maatschappelijke en technische opgaven van een oplossing te voorzien. Ook kan ze voortkomen uit de opvatting dat de wereld niets anders is dan een stroom data en dat we met digitalisering dus pas echt grip krijgen op de werkelijkheid (dataïsme).

⁵ Egbert Schuurman, *Transformation of the Technological Society* (Dordt: Dordt Press, 2022), 37.

Ten slotte, in de meest extreme zin kan er een defaitistische houding ontstaan richting digitalisering. Men kan haar zien als de volgende noodzakelijke stap van intelligentie en bewustzijn, waarin de mens ondergeschikt raakt aan een hogere vorm van intelligentie die nu gebouwd wordt door supercomputers, het zogenoemde moment van singularity, of in goed Nederlands: singulariteit. In deze houding zien we een overwaardering van de rekenkracht van machines, de beperking van intelligentie tot die rekenkracht, en de reductie van ons mensbeeld tot een domme computer, met alle beperkte rechten van dien. We noemen kort de voornaamste drie bezwaren hiertegen. Gelovigen menen dat ieder mens onvoorwaardelijk het recht tot leven heeft, en dat ieder mens, ongeacht zijn of haar IQ of rationaliteit, waardevol is. En intelligentie op zichzelf is niet wat te prijzen valt in menselijk gedrag, maar moreel denken en handelen wel, wat het Spreukenboek 'wijsheid' noemt. Moreel denken en gedrag kan niet door een algoritme aangeleerd worden, onze morele waarden (of gebrek eraan) kunnen wel tot uiting komen in opdrachten aan computerprogramma's.

Cultiveren (rentmeesterschap)

In plaats van het afwijzen, het neutraal benaderen of omarmen van digitale technologieën, zien we in het cultiveren van digitale technologie een houding die past bij de opdracht uit Genesis 2:15 om de aarde als rentmeester te bewerken en te bewaren. We mogen, ons bewust van onze tekortkomingen, aan de slag in deze wereld en digitale technologieën, terwijl we verantwoordelijkheid dragen voor God, elkaar en onszelf. De verworvenheden van techniek zijn velerlei, van de dijken en Deltawerken tot vaccins en riolering. Techniek kan de samenleving helpen en daar mogen we dankbaar voor zijn, ook richting onze Schepper.

We kunnen dus digitale technieken gebruiken om de aarde te bebouwen en te bewaren, maar we blijven zelf niet buiten schot. Ook onze eigen omgang met digitalisering moet onderwerp zijn van cultivering en herijking. We zullen keuzes moeten maken en grenzen moeten aangeven in digitale toepassingen, zowel in de samenleving als in de politiek. We zullen ons als samenleving en overheid bij elke bruikbare digitale toepassing die we inzetten, moeten oefenen in het gebruik ten goede.

Waardevol en begrensd

In deze inleiding hebben we toegelicht in welke denktraditie de ChristenUnie staat op het gebied van digitale technologie en digitalisering. Het is een traditie die digitalisering op waarde wil schatten en niet bij voorbaat af wil wijzen. Tegelijk is onze denktraditie niet overoptimistisch over het gebruik van digitale technologieën omdat die ontwikkeld en gebruikt worden in een imperfecte wereld door onvolmaakte mensen. Dat gegeven moet ons alert maken op de misstanden die kunnen ontstaan door onbegrensde digitalisering, temeer omdat digitale technieken geen randverschijnsel in de samenleving zijn, maar juist steeds meer centraal staan in hoe we werken, leven en het openbaar bestuur vormgeven. Politici van de ChristenUnie hebben publieke gerechtigheid als inzet van hun handelen. Ze hebben daarmee de verantwoordelijkheid om de ontwikkelingen te analyseren en zo nodig via overheidshandelen in te grijpen waar gerechtigheid en menselijke waardigheid tekortgedaan worden in digitale processen. Vanuit deze denktraditie kunnen we ons richten op de waarden en uitgangspunten van de ChristenUnie die van belang zijn voor digitaliseringsvraagstukken.

Leestips over (digitale) techniek, samenleving en christendom

Jacques Ellul geeft in *The Technological Society* een doordenking van onze maatschappij vanuit christelijk filosofisch perspectief. Hij laat zien dat onze (over)waardering van technologie leidt tot een vorm van technologisch denken waarin we technologie als de oplossing zien van onze problemen.

In de uitgave van Groen 'Kunstmatige Intelligentie: Computer says no' (maart 2021, Wetenschappelijk Instituut ChristenUnie) doordenken ChristenUnieleden de betekenis van kunstmatige intelligentie voor ons politieke handelen.

Voor een overzicht van de filosofie van techniek, zie: Maarten J. Verkerk, Jan van der Stoep, Jan Hoogland, Marc J. de Vries, *Denken, Ontwerpen, Maken. Basisboek Techniekfilosofie* (Amsterdam: Boom, 2007).

Een overzicht van kunstmatige intelligentie en enkele reflecties erop door christenwetenschappers worden gegeven in 'Artificiële Intelligentie. Tussen feit en fictie', In: Radix, Tijdschrift over geloof, wetenschap en samenleving, Uitgave ForumC, Jaargang 48 #2, 2022.

Voor een Engelstalig boek over digitalisering vanuit christelijk perspectief, zie: Derek C. Schuurman, *Shaping a Digital World: Faith, Culture and Computer Technology*, (Westmont: IVP Academic, 2013).

Hoofdstuk 2. Waarden vanuit de beginselverklaring

De ChristenUnie is een beginselpartij, wat inhoudt dat onze partij een aantal 'beginselen' of uitgangspunten heeft die de basis van onze politiek vormen. De beginselen van de ChristenUnie staan in de Beginselverklaring (2018). Sommige van die beginselen zijn specifiek voor christelijke politiek, zoals 'soevereiniteit in eigen kring' en 'gebrokenheid'; andere zijn veel algemener, zoals 'democratische rechtsstaat' en 'onpartijdige overheid'. Dit hoofdstuk van de digitaliseringsvisie van de ChristenUnie kiest uit de Beginselverklaring enkele uitgangspunten die juist rondom digitalisering belangrijk zijn. Zoals toegelicht in de inleiding benaderen we digitalisering daarbij niet afwijzend, omarmend of onverschillig, maar vanuit de wens digitalisering te cultiveren.

Niet alle uitgangspunten zijn op alle vraagstukken van toepassing. We hebben gekozen voor een indeling in drie delen. Met deze indeling hopen we eraan bij te dragen dat digitaliseringsvraagstukken door de ChristenUnie beoordeeld worden op 1) de rol van de overheid in een vraagstuk, 2) de omgang met mensen en menselijkheid in digitaliseringsvraagstukken en 3) de impact van digitalisering op ons samenleven.

Deze uitgangspunten zijn niet bedoeld als een beslisboom – in dat geval hadden we er wel een app van gemaakt – het zijn uitgangspunten die we voorhouden aan ChristenUniepolitici in de hoop dat ze helpen bij het beoordelen van digitaliseringsvraagstukken in de praktijk. Daarbij schuwen we grote woorden als 'macht' en 'vrede' niet, omdat we naast de technische vormgeving van digitale systemen ook de richting en de gevolgen ervan niet uit het oog willen verliezen.

De uitgangspunten uit het beginselprogramma zijn voorzien van een toespitsing op digitaliseringsvraagstukken. De toespitsing is niet het enige wat erover te zeggen valt, maar beoogt een begin te zijn bij het verder doordenken van ChristenUnieuitgangspunten bij concrete digitaliseringsvraagstukken. In het derde hoofdstuk zullen we de toepassing van deze waarden op concrete vraagstukken illustreren aan de hand van een aantal casussen en afwegingen. Met deze indeling hopen we eraan bij te dragen dat digitaliseringsvraagstukken door de ChristenUnie beoordeeld worden op 1) de rol van de overheid in een vraagstuk, 2) de omgang met mensen en menselijkheid in digitaliseringsvraagstukken en 3) de impact van digitalisering op ons samenleven. Zie Figuur 1 voor een overzicht deze drie 'pijlers' en de bijbehorende waarden.



Figuur 1: waardenmodel

2.1. Uitgangspunten voor overheidshandelen in digitaliseringsvraagstukken

Verantwoordelijkheid – Macht draait om verantwoordelijkheid nemen. We zijn geroepen macht dienstbaar te maken aan recht.

Een van de aspecten van digitalisering is dat beslissingen meer geautomatiseerd plaatsvinden. Besluiten worden verplaatst van het menselijke terrein naar het machinedomein. De systemen worden door experts gemaakt; de werking en implicaties daarvan voor politiek en bestuur zijn nog niet uitgekristalliseerd.

- Verantwoordelijkheid nemen: machines kunnen geen verantwoordelijkheid dragen. Daarom zijn mensen eindverantwoordelijk bij overheidsbesluiten die geautomatiseerd worden voorbereid. Verantwoordelijken moeten ook aanspreekbaar en bereikbaar zijn.
- Verantwoordelijkheid nemen betekent ook dat overheidshandelen uitlegbaar moet zijn. Dat stelt eisen aan de inrichting van geautomatiseerde systemen.

Begrenzing – Macht wordt begrensd door recht, tegenmacht en verantwoording. Juist op een plaats waar macht samenbalt, is het kwaad gevaarlijk. De overheid moet daarom haar grenzen kennen, zichzelf inperken en ingeperkt worden.

Digitalisering biedt overheden veel mogelijkheden om het openbaar bestuur vorm te geven. Veel processen kunnen beter, inzichtelijker, sneller, slimmer, efficiënter en goedkoper wanneer ze digitaal vormgegeven worden – wie kan daar tegen zijn? In de speciale relatie tussen overheid en burger mogen ze toch niet doorslaggevend zijn. Recht, tegenmacht en verantwoording vormen ijkpunten van overheidshandelen: zij begrenzen digitalisering in het overheidsdomein. De toeslagenaffaire maakt pijnlijk duidelijk dat macht niet zonder recht kan. Zowel de vormgeving van digitale processen binnen de overheid zelf als het overheidsoptreden in de digitale samenleving vraagt om evenwichtskunst in optreden en terughoudendheid.

- Middels het recht kunnen overheden marktpartijen begrenzen. Wetgeving met betrekking tot digitalisering moet verder ontwikkeld worden in een digitaliserende samenleving zodat de 'digitale ruimte' niet vanzelf toevallt aan het recht van de sterkste.
- Digitalisering biedt overheden meer mogelijkheden om te surveilleren en gedrag te beïnvloeden en te sturen. Dat kan ook zijn richting positieve beleidsdoelen als verbetering van veiligheid en gezondheid of de beperking van de uitstoot van broeikasgassen. Daar dient de overheid niet de mogelijkheden maar het recht en de waardigheid van mensen als uitgangspunt te nemen. Juist waar mogelijkheden onbegrensd lijken, moet de overheid zichzelf kunnen begrenzen.

Soevereiniteit in eigen kring – De overheid neemt de verantwoordelijkheid van andere maatschappelijke verbanden niet over. Zij beschermt hun ruimte om hun verantwoordelijkheid te kunnen nemen en ondersteunt hen in die verantwoordelijkheid.

Digitalisering voegt een nieuwe dimensie toe aan de samenleving en dat vraagt om herijking van de verantwoordelijkheid tussen overheid, samenleving en markt. Het uitgangspunt van soevereiniteit in eigen kring is, dat de overheid de samenleving ondersteunt en dat de verschillende sectoren of verbanden in de samenleving een eigen ruimte en doel hebben. De gedachte dat de overheid die verbanden ondersteunt maar niet 'overneemt', geldt ook in het digitale domein.

- Net als het marktplein in de 'analoge wereld', dat bevolkt wordt door ondernemers en bezoekers, bewaakt de overheid vanuit haar recht de digitale ruimte, maar eigent zich die niet toe omdat de overheid daar niet het recht toe heeft. Dit geldt voor de online ruimte en voor de infrastructuur van het internet. De digitale ruimte is niet het

- eigendom van een partij. Niet van een commerciële partij, niet van een overheid, niet van een persoon.
- Aanbieders van digitale diensten kunnen een grote invloed hebben op domeinen als zorg en onderwijs. Het is niet wenselijk dat beslissingen die thuishoren in zorg en onderwijs zo sterk gestuurd worden door commerciële (tech)aanbieders, dat de eigenlijke taak van die domeinen geschaad wordt.⁶

Publieke gerechtigheid – Recht beschermen en handhaven. De overheid waakt over de ordening van de samenleving en het gemeenschappelijk belang. Zij beschermt het kwetsbare en de kwetsbaren.

- Rechtsbescherming en handhaving gaan niet per se hand in hand met principes die de basis van digitalisering vormen: kostenbeheersing, effectiviteit en efficiency, innovatie en productiviteit. Sturing met het oog op de waarden van publieke gerechtigheid is daarom nodig.
- Vergaande digitalisering maakt wie niet digitaal vaardig is kwetsbaar voor uitsluiting en maakt iedere internetgebruiker kwetsbaar voor uiteenlopende risico's, van profiling tot grooming, van socialemidiaverslaving tot spyware. Publieke gerechtigheid vraagt evenwichtskunst van overheden in het stellen van online grenzen zonder daarbij zelf grenzeloos op te treden.

Moreel bestuur – De overheid is niet neutraal, maar zoekt wat goed is. Leiders dienen ook morele leiders te zijn door recht en onrecht te benoemen. Ze zijn eerlijk over de beperkte reikwijdte van politiek.

Ook digitalisering moet ingebed zijn in een zoektocht naar wat goed is om te doen. Wat het goede is, is niet altijd makkelijk te ontwaren. Dat geldt voor politiek in het algemeen en ook voor digitaliseringsvraagstukken. Effecten van digitalisering kunnen verschillend uitpakken en zijn niet altijd te voorzien of te evalueren. Van moreel bestuur mogen we ten minste verwachten dat het openstaat voor een moreel gesprek over digitale toepassingen in het publieke domein.

- Moreel bestuur neemt verantwoordelijkheid voor de systemen die onder haar bestuur gebruikt worden.
- Digitale systemen hebben geen moreel kompas, geweten of op een andere manier een zelfstandige oriëntatie op goed of kwaad. Daarom moet het gebruik ervan ingebed worden in een morele context. Ethiek dient een centrale plaats te hebben bij ontwerp en toepassing.
- Moreel bestuur zoekt wat goed is. Digitale innovatie kan een goed doel hebben maar digitalisering is in het openbaar bestuur geen doel op zichzelf en evenmin een wedstrijd.

Internationale gerechtigheid en soevereiniteit – Internationale samenwerking kan bijdragen aan recht en vrede wereldwijd, maar mag niet uitmonden in een concentratie van macht en dient de soevereiniteit niet te verzwakken.

Digitalisering bevordert internationale samenwerking. Door digitalisering vervagen grenzen en kan informatie snel en tegen lage kosten worden verspreid. Digitalisering kan bijdragen aan recht en vrede, zoals wanneer minder ontwikkelde gebieden toegang krijgen tot informatie en publieke voorzieningen.

⁶ Onderwijsraad, *Doordacht digitaal* (Den Haag: Onderwijsraad, 2017) 23-24.

Digitalisering bedreigt tegelijkertijd de soevereiniteit van overheden als zij door een gebrek aan afgrenzing hun taken niet kunnen uitvoeren of buitenlandse statelijke of commerciële actoren ongewenste invloed uitoefenen op burgers.

- De overheid belemmert de inzet van digitalisering bij het nastreven van internationale gerechtigheid niet.
- De overheid stelt binnen het digitale domein grenzen die nodig zijn ter bescherming van de soevereiniteit van de Europese, nationale, provinciale of lokale gemeenschap, om de uitvoering van overheidstaken mogelijk te maken en om burgers af te schermen tegen ongerechtvaardigde beïnvloeding door buitenlandse actoren.

2.2. Menselijke waarden in digitale tijden

Persoonlijke levenssfeer (privacy) – Mensen hebben recht op een persoonlijke levenssfeer.

In tijden van digitalisering staat onze privacy sterk onder druk. Er zijn bedrijven, overheden en mensen die intieme informatie als object van handel of manipulatie gebruiken. De overheid beschermt burgers door hun persoonlijke levenssfeer te beschermen en burgers hebben daarin ook een eigen verantwoordelijkheid. Grootschalige dataverzameling van persoonsgegevens brengt met zich mee dat de kans op datalekken structureel toeneemt. Dat gegeven zou terughoudend moeten maken in het verzamelen en bewaren en delen van persoonlijke gegevens die ook ten kwade gebruikt kunnen worden. Tegelijk is aandacht nodig voor situaties waarin privacywetgeving belemmerend werkt bij het geven van hulp aan wie dat nodig heeft.

- De overheid moet zelf de persoonlijke levenssfeer respecteren, juist omdat de band tussen overheid en burger geen kwestie van vrije keuze is.
- Digitale verdienmodellen waarin het delen van data (financieel) voordeel oplevert, bedreigen de persoonlijke levenssfeer.

Relationeel bestaan (verbondenheid en solidariteit) – We komen tot bloei niet in lege autonomie maar in ons samenleven. We leven in afhankelijkheid van anderen. Een goed leven is een leven in verbondenheid.

Digitalisering kan zowel verbinden als vervreemden. De samenleving kan alleen samenleving zijn als mensen elkaar blijven ontmoeten. Dat kan digitaal, maar kan niet uitsluitend digitaal. We mogen van zowel overheidspartijen als marktpartijen vragen dat ze zich, naast de effecten op individuen, ook rekenschap geven van wat de inzet van digitale toepassingen doet met de samenleving in haar geheel en gemeenschappen en verbanden in de samenleving.

- Er zijn voor beleid en producten kwaliteitsstandaarden, impactanalyses, keurmerken en juridische kaders ontwikkeld, denk aan de milieueffectrapportage en het voorzorgbeginsel. Wenselijk zou de ontwikkeling zijn van zoiets als een sociaal-maatschappelijke impactanalyse ex ante, waarin aanbieders van maatschappelijk impactvolle digitale technologie (denk aan de invloed van ChatGPT op het onderwijs), zich rekenschap geven van te verwachten gevolgen op aspecten van brede welvaart (gezondheid, onderwijs, milieu en leefomgeving, sociale cohesie, persoonlijke ontplooiing en (on)veiligheid en effecten op mensen ergens anders en generaties na ons.) Vervolgens kan achteraf een maatschappelijk gesprek plaatsvinden over maatschappelijke kosten en baten van een toepassing. Het gaat daarbij niet zozeer om een juridische insteek maar eerder om een instrument om aanbieders en samenleving bij elkaar te betrekken.
- Omdat digitalisering de manier van samenleven raakt, is het nodig dat we ook als

samenleving in gesprek blijven over wat we wel en niet willen. Terwijl een wettelijk verbod op een toepassing mogelijk moet zijn, is dat niet altijd de beste route. Hier geldt een analogie met de niet-digitale wereld, waar ook dingen gebeuren die niet wenselijk zijn en waarover verschillende opvattingen mogelijk zijn.

Veiligheid – Bescherming van de veiligheid van haar burgers is een kerntaak van de overheid.

Terwijl traditionele criminaliteit afneemt, groeit digitale criminaliteit flink en zijn ook nationale veiligheidsbelangen in het geding. Analooq aan het niet-digitale domein kan de overheid veiligheid niet garanderen, maar moet zij wel haar verantwoordelijkheid nemen. Veiligheid kan niet anders dan een gezamenlijke inspanning zijn van overheid, markt en samenleving.

- Vanwege de unieke (verplichte) relatie tussen overheid en burger is databeveiliging en data-ethiek bij overheden cruciaal.
- Ook burgers hebben een verantwoordelijkheid in het voorkomen van digitale criminaliteit. We zetten onze fiets op slot en doen ook onze digitale deur dicht tegen ongewenst bezoek.
- Het is onwenselijk een veiliger samenleving te maken die vooral leunt op sterke inzet van digitale surveillance in het fysieke domein. De samenleving is gebaat bij veiligheid die ontstaat in medemenselijkheid. We zoeken weerbaarheid uiteindelijk in de publieke moraal die blijft bestaan wanneer de veiligheidscamera uitvalt.

Gelijkheid – Burgers zijn gelijk voor de wet.

Hoewel digitalisering kansen biedt om kansengelijkheid tegen te gaan zijn er ook aanwijzingen dat digitalisering ongelijkheid in de praktijk juist vergroot. Rondom digitalisering is gelijkheid dus een belangrijk aandachtspunt.

- Ongelijke behandeling op basis van onjuiste, irrelevante of oude data past niet bij het uitgangspunt dat burgers gelijk zijn voor de wet.
- In de ontwikkeling van nieuwe systemen en spullen, dient er nagedacht te worden over verschillende soorten gebruikers. (Voorbeeld: er zijn digitale systemen die bepaalde huidskleuren niet herkennen/ algoritmen die door onjuiste data (onbewust) discriminerend werken.)
- Gelijkheid betekent ook rekening houden met wie wel wil maar wie het niet lukt om mee te komen in de digitale samenleving.

Ethiek van leven – De ethiek van het leven leidt onze technologische ontwikkeling in onder andere de zorg – en niet omgekeerd. De mens is geschapen als kroon op de schepping. We zijn geroepen het menselijk leven te beschermen.

Nieuwe digitale ontwikkelingen kunnen beloven het leven van mensen makkelijker, gezonder en socialer maken. Tegelijkertijd is het verkeerd om mensen als optimalisatie-objecten te beschouwen. Hierdoor kan het idee ontstaan om gezonde mensen onnodig te 'optimaliseren'. Digitalisering kan het leven verbeteren, maar het leven hoeft niet optimaal te zijn.

- Over mensen kunnen gegevens worden verzameld en mensen produceren gegevens, maar mensen zijn meer dan een verzameling gegevens. De waardigheid van mensen is groter dan die datawaarde.

2.3. Samenlevingsdoelen in tijden van digitalisering

Duurzaamheid – We dienen allen met kracht te kiezen voor duurzaam handelen. Duurzame keuzes staan tegenover het uitputten van onze leefomgeving en die van anderen.

Het digitale leven lijkt soms over een niet-materiële werkelijkheid te gaan: internetverkeer en de cloud lijken in de lucht te hangen en daarmee los te staan van duurzaamheidsvraagstukken. Maar dat is schijn: digitaliseringsvraagstukken gaan ook over grondstoffen, mensenrechten en de uitstoot van broeikasgassen.

- Digitalisering kan niet zonder materie: hardware bestaat uit onder meer zeldzame (conflict) mineralen. De winning van grondstoffen en assemblage van hardware gebeurt vaak in slechte werkomstandigheden. De training van datamodellen vindt vaak plaats via slechtbetalende gig-platforms.
- Digitale technologie kan bijdragen aan het halen van duurzame doelen, maar is – net als technologie in veel andere sectoren – vooralsnog vooral vervuilend in alle fases, van productie tot afdankfase.
- De belofte van vergroening wordt geen werkelijkheid zonder keuzes voor duurzaamheid in digitalisering en sturing op uitstootvermindering.⁷ Zonder die sturing leidt digitalisering tot meer uitstoot van broeikasgassen.

Genieten van genoeg – Genieten van genoeg, tegenover honger naar altijd meer produceren en consumeren.

Het hoort bij mensen om de wereld door techniek te bewerken. Digitalisering daagt mensen uit om systemen in te richten, te optimaliseren en slim te maken. Het is indrukwekkend wat mensen met techniek kunnen bereiken.

Toch kan – zoals bij alles – een teveel van het goede in haar tegendeel resulteren. Daarom waken we voor de gedachte dat meer digitalisering per definitie altijd beter is en dat digitalisering de oplossing voor elk (maatschappelijk) probleem biedt.

- Data zelf zijn grenzeloos: eindeloos beschikbaar en te delen. Elke minuut wordt er voor 300 uur aan videocontent geupload op platform YouTube. Maar bij genieten van genoeg hoort de waarde van rust: we hoeven niet altijd online, 'aan' en bereikbaar te zijn.
- We zouden honger naar gegevens en datagedreven systemen kunnen zien als de digitale evenknie van honger naar altijd meer produceren en consumeren. Net als produceren en consumeren op zichzelf niet verkeerd zijn maar wel ongezonde trekken kunnen krijgen, kan dat met het verzamelen van gegevens en het benaderen van de wereld als een data-werkelijkheid gebeuren. Er is meer in het leven dan spullen kopen – en er is een wereld die we niet in systemen en gegevens kunnen en willen vangen. Het is goed om ook offline te leven. Ook in digitaliseringsvraagstukken willen we leren te genieten van genoeg.

Vrijheid – Mensen hebben de vrijheid gekregen om vanuit hun diepste geloof en overtuigingen keuzes te maken in het leven. We zijn geroepen elkaar in deze vrijheid te laten delen.

In de praktijk blijkt dat digitalisering zowel vrijheid kan vergroten als verkleinen, waarbij er tussen landen grote verschillen zijn. Zo kunnen mensen in Nederland door sociale media in vrijheid hun mening ventileren, maar staat het gure online klimaat een open publiek debat in de weg.

- Digitalisering biedt nieuwe mogelijkheden voor nudging, oftewel subtiele

⁷ Raad voor de Leefomgeving, *Digitaal Duurzaam* (Den Haag: RvdL, 2021) 14-15.

gedragsbeïnvloeding. Het uitgangspunt dat mensen in vrijheid naar hun geloof en overtuigingen keuzes mogen maken, staat op gespannen voet met nudging wanneer die 'op maat gemaakt' is op basis van persoonlijke gegevens.

Democratisering – Democratisering nodigt iedereen uit om de richting mee te bepalen en streeft ernaar dat iedere stem gehoord kan worden.

Vergaande digitaliseringsbesluiten moeten in een open publiek en politiek debat besproken worden zodat we als samenleving democratisch gedragen keuzes kunnen maken.

- Digitale toepassingen kunnen, al dan niet bedoeld, democratisering versterken of verminderen.
- Digitaliseringsmarkten tenderen naar monopolievorming. Doorgaande accumulatie van kennis en macht hindert democratisering.
- In overheidstoepassingen (en breder) is het van belang dat trainingsdata voor algoritmes breed getraind zijn om bias en buitensluiting (of niet terechte opsporing) te voorkomen.

Hoofdstuk 3. Afwegingen en richtlijnen

In dit hoofdstuk bespreken we een aantal specifieke situaties waarin (politieke) afwegingen gemaakt kunnen worden. De onderwerpen starten met een casus die het thema illustreert, waarbij we de gebruiker centraal stellen. Voor ieder onderwerp laten we zien hoe de waarden die in het vorige hoofdstuk zijn besproken gebruikt kunnen worden om een afweging te maken. We sluiten ieder onderwerp af met een aantal richtlijnen die uit de afwegingen afgeleid kunnen worden.

Per onderwerp geven we aan voor welke politieke gremia het thema relevant is: Europees Parlement (EP), Eerste Kamer (EK), Tweede Kamer (TK), Provinciale Staten (PS), Waterschappen (WS), en/of gemeenteraden (GR).

3.1. Gepersonaliseerde advertenties

Relevant voor: EP, EK, TK

Casus

Truus uit Oldenburger is vandaag vroeg wakker. Ze gaat maar even de krant lezen. Uiteraard digitaal, op papier is niet meer van deze tijd. Handig ook, met een duimpje kun je aangeven dat je een artikel leuk vindt of met wegschrijven dat het niets voor je is. Zo krijg je altijd gepersonaliseerd nieuws, speciaal voor jou. Het is een lerend systeem. O kijk, daar staat de advertentie waar mijn vriendin het gisteren over had. Die elektrische fiets van 1700 euro, maar bij mijn vriendin was die maar 50 euro. Per maand natuurlijk. Zij zou een groot bedrag niet in een keer kunnen betalen. Wel handig dat het systeem daar rekening mee houdt, zou het weten waar ze woont? Was wel grappig, pas had ik allemaal datingadvertenties. Kwam er later pas achter dat het profiel nog op mijn man stond toen ik de krant las. Schijnt dat alle mannen in die leeftijd dergelijke advertenties krijgen. Heeft in ieder geval niets te maken met zijn zoekgedrag op internet, zei hij. Hoewel, toen we pas naar vakanties hadden gekeken, kreeg ik ineens allemaal aanbiedingen van huisjes. Of valt dat ineens meer op omdat je met de vakantie bezig bent? Hoe dan ook, het heeft toch vooral voordelen. Neem nu die schoenenadvertentie. Bestelde ik maat 38, gaf de site het advies maat 39 te nemen. Vond zo'n grote maat gênant, maar toch maar besteld. En wat denk je? Paste perfect! Alleen, nee toch, heb je weer zo'n advertentie van de ChristenUnie. Dat heb je als je als vrouw van rond de veertig in deze regio woont. Daar word je dan wel weer een beetje simpel van... Weten ze dan niet dat ik allang ChristenUnie stem?

Afweging van waarden

Het personaliseren van diensten heeft duidelijk twee kanten. Aanbieders proberen beter aan te sluiten bij behoeften van (potentiële) klanten vanuit commercieel perspectief. Als gebruiker is het prettig dat je je voorkeuren kunt instellen voor het nieuws waarin je bent geïnteresseerd, en is het handig wanneer een systeem deze voorkeuren automatisch leert. Het voelt wat ongemakkelijker als je in de auto stapt en je telefoon je vertelt dat er een file staat op weg naar je bestemming en je beter een andere route kunt nemen. Dat wil zeggen, het advies is prettig, maar hoe weet mijn telefoon waar ik heenga? Het wordt nog ingewikkelder als commerciële ondernemingen in wijken waar veel huishoudens schulden hebben, producten aanbieden op afbetaling en in rijke wijken niet. Dit schuurt met publieke gerechtigheid omdat kwetsbare inwoners in de verleiding worden gebracht zich nog verder in de schulden te steken.

Iedereen is in ieder geval vrij, toe te staan, dat persoonsgegevens worden gebruikt door bedrijven en organisaties om persoonlijke aanbevelingen te doen. Maar pas op, hoe vrij zijn we werkelijk? Als je op je telefoon een vinkje aan moet klikken waarmee je toestemming geeft voor het gebruik van je locatie, besef je dan waarvoor je toestemming geeft? Zeker als er een vinkje moet worden gezet onder de gebruiksvoorwaarden die pagina's lang zijn, misschien zelfs in een andere taal. Denk je wellicht dat

je anders je nieuwe telefoon niet kunt gebruiken? Transparantie is in ieder geval belangrijk. Duidelijk moet zijn waarom je een specifieke aanbeveling krijgt, bijvoorbeeld vanwege de voorkeuren die je zelf hebt aangegeven (bijvoorbeeld dat je het regionale nieuws wilt ontvangen, en sportnieuws en juist geen economisch nieuws). Ook bij ingewikkelde algoritmen moeten keuzes te herleiden zijn (explainable AI), zodat er ook kan worden gecontroleerd op discriminatie.

Bij het opstellen van een persoonlijk profiel van een internetgebruiker gaat het over privacy. De ChristenUniebeginselverklaring zegt daarover: 'De overheid beschermt burgers door hun persoonlijke levenssfeer te beschermen'. De overheid beschermt dus tegen het verzamelen en verwerken van persoonsgegevens – inclusief het opstellen van profielen – als burgers dat niet willen. Ook zou er, net als bij alle persoonlijke dossiers, inzagerecht en recht op verwijdering moeten worden geregeld.

Ten slotte speelt de vraag hoe gepersonaliseerde advertenties zich verhouden tot de democratische rechtsstaat en goed samenleven. Een goede markt draait om de bloei van mensen. Mensen komen niet tot bloei als hun keuzemogelijkheden worden ingeperkt door gerichte advertenties. Hiermee wordt de macht van bedrijven (en overheid) vergroot ten koste van keuzevrijheid. Persoonlijke advertenties en nieuwsberichten kunnen zelf leiden tot een steeds nauwere 'informatiebubble', wat in het uiterste geval kan leiden tot radicalisering, waarbij alternatieven, inkeer en nieuwe inzichten steeds verder uit het zicht raken. We kunnen slechts samenleven als we in een gedeelde werkelijkheid leven. Gepersonaliseerde advertenties en nieuwsberichten mogen niet leiden tot afgescheiden leefwerelden en een gepolariseerde samenleving.

Conclusie

Het afstemmen van bedrijven op behoeftes van de klant is van alle tijden. Bij de digitale variant is het goed om op een aantal randvoorwaarden te letten. Keuzevrijheid, zowel om gepersonaliseerde informatie te krijgen, als om juist niet speciaal voor jou gefilterde informatie, moet worden gegarandeerd. Naast de voorwaarde dat gepersonaliseerde informatie en aanbiedingen herkenbaar zouden moeten zijn als gepersonaliseerd, is het ook belangrijk dat inzichtelijk is hoe de selectie heeft plaatsgevonden. In het geval van AI-gedreven personalisatie kunnen er dus randvoorwaarden gesteld worden aan het algoritme (explainable AI). De overheid dient haar burgers te beschermen tegen het misbruiken van personalisatietechnieken. Ze dient er tevens rekening mee te houden dat personalisatie kan leiden tot verkokerde opvattingen. Internetgebruikers dienen zelf te kunnen bepalen welke gegevens ze wel of niet beschikbaar stellen aan anderen voor personalisatie.

3.2. Toegankelijkheid digitale wereld (en recht op niet-deelname)

Relevant voor: EP, EK, TK, PS, WS, GR

Casus

David helpt regelmatig zijn oude buurvrouw Annelies met bankzaken, contracten en de communicatie met de overheid. Annelies heeft weliswaar een computer en deed een paar jaar geleden een computercursus, maar handigheid met de computer en het internet heeft ze nooit gekregen. Tegen David verzucht ze dat tegenwoordig alles maar via het internet moet: internetbankieren, informatie van de overheid, contracten van de energiemaatschappij – het wordt vaak alleen via het internet aangeboden. Als David haar niet zou helpen, wist Annelies niet hoe ze haar zaken nog kon regelen. Die hulp wordt er overigens niet makkelijker op. Een wachtwoord delen is niet meer genoeg. David heeft vanwege de tweestapsauthenticatie steeds vaker de telefoon van Annelies nodig. Aan de andere kant van David woont Sven. Sven is een dertiger die heeft besloten om volledig analoog te leven. Hij heeft geen computer en geen smartphone meer. Sven klaagt regelmatig bij David dat het steeds minder wordt geaccepteerd dat hij niet digitaal communiceert. Laatst belde hij voor een afspraak met de tandarts en werd de receptioniste boos op hem, omdat hij niet via het internet een afspraak had gemaakt. Toen hij

in verband met zijn zorgtoeslag een loonsverhoging wilde doorgeven, heeft hij een uur lang in de wacht gestaan bij de Belastingdienst. Sven vindt dat hij het recht heeft om 'analoog' te blijven leven, en dat de overheid en bedrijven hem die mogelijkheid moeten blijven bieden.

Afweging van waarden

Als samenleving maken we gebruik van digitale middelen en technieken om informatie te verstrekken, met elkaar te communiceren en producten en diensten aan te bieden. Denk aan informatie op websites, aan communicatie via e-mail, digitale formulieren en DigiD, en aan online consulten met een psycholoog of de abonnementen op digitale video- en muziekdiensten. Onderdeel zijn van een samenleving betekent dat we niet altijd vrij kunnen kiezen welke middelen we gebruiken om informatie te vergaren, te communiceren en gebruik te maken van producten en diensten. We zijn soms gebonden aan de keuzes die anderen voor ons maken. Een ChristenUniewaarde als goed samenleven betekent dat de keuzes die door anderen worden gemaakt soms moeten worden aanvaard. Degene die zijn autonomie koste wat het kost wil bewaren, zondert zich af van de samenleving. De principiële keuze om niet mee te doen aan de digitale samenleving kan tot op zekere hoogte worden gerespecteerd, maar hoeft niet oneindig te worden gefaciliteerd. De digitale registratie van bepaalde basisinformatie is bovendien onvermijdelijk voor elke burger. Zonder digitale registratie van onder meer geboorte, huwelijk, overlijden – en ook van adres en burgerservicenummer – kan iemand geen onderdeel zijn van de samenleving. Dus ook wie zelf niet digitaal actief is, kan niet eisen hij niet voorkomt in digitale systemen.

Toenemende digitalisering levert toenemende ongelijkheid op voor wie niet kan of wil digitaliseren: er ontstaat een digitale kloof. Samenleven betekent dat rekening wordt gehouden met de mogelijkheden die eenieder heeft om mee te kunnen doen. Het gebruik van digitale middelen en technieken vergt bepaalde fysieke en mentale mogelijkheden, vergt bepaalde kennis en vaardigheden en vergt bepaalde digitale middelen. Mensen met fysieke handicaps, mentale problemen, verstandelijke beperkingen, gebrekkige vaardigheden en/of beperkte financiële mogelijkheden kunnen niet altijd meedoen. Een hier relevante ChristenUniewaarde is sociaal beleid. Die houdt in dat de overheid erop toeziet dat iedereen mee kan doen. Essentiële overheidsdiensten moeten voor iedereen toegankelijk zijn. De wijze waarop de overheid hiervoor zorgt, is afhankelijk van de belemmeringen waar bepaalde burgers tegenaan lopen. Ruim twee miljoen Nederlanders boven de zestien jaar zijn niet geletterd genoeg om makkelijk met de samenleving mee te komen. De problemen in geletterdheid werken door in de omgang met digitalisering. Voor laaggeletterde burgers, nieuwkomers en slechtzienden kan het noodzakelijk zijn in eenvoudige taal online informatie aan te bieden. Voor ouderen met geringe digitale vaardigheden kan de instandhouding van fysieke loketten worden gecombineerd met het aanbieden van toegankelijke hulp en (computer)cursussen. Voor mensen die blind zijn kan het noodzakelijk zijn om informatie auditief aan te bieden. Burgers zonder computers, zonder internet of zonder de juiste software moeten tegen geringe kosten een plek krijgen waar zij digitaal kunnen communiceren, zoals openbare bibliotheken waar de e-mail kan worden bekeken en beantwoord of kan worden gewerkt aan schoolopdrachten.

Hulp bij gebruik van digitale middelen en technieken kan ook worden geboden door medeburgers. Dit kan soms lastig zijn, omdat wachtwoorden en toegangscode's persoonsgebonden zijn. Hulp op afstand wordt bemoeilijkt als voor het inloggen zowel een wachtwoord als een aanvullende inlogcode nodig is. Dit soort strenge beveiliging helpt tegen fraude, maar werpt tegelijkertijd een drempel op voor eenvoudige hulp. De uitdaging is om digitaal minder vaardige burgers eenvoudig hulp te kunnen geven, zonder dat zij daarmee makkelijk slachtoffer worden van misbruik of hun autonomie volledig uit handen moeten geven.

De overheid neemt de verantwoordelijkheid van andere maatschappelijke verbanden niet over. Uit de ChristenUniewaarde soevereiniteit in eigen kring volgt dat elk maatschappelijk verband eigen verantwoordelijkheden heeft. Bedrijven en organisaties mogen zelf bepalen of, en zo ja, hoe zij het gebruik

van digitale middelen en technieken faciliteren voor mensen die niet mee kunnen doen. De overheid kan bedrijven en ondernemingen ondersteunen bij het nemen van hun verantwoordelijkheid, maar neemt die verantwoordelijkheid niet over. Zo kunnen bedrijven en organisaties bijvoorbeeld niet gedwongen worden analoog te communiceren, tenzij zij diensten leveren die cruciaal zijn voor burgers om behoorlijk te kunnen leven. Denk aan de levering van elektriciteit en gas. Bedrijven en ondernemingen die dit soort cruciale diensten aanbieden en die hun verantwoordelijkheid niet nemen, kunnen wel worden gedwongen om analoge diensten aan te bieden.

De overheid beschermt de veiligheid van burgers. Juist bij burgers die minder digitale mogelijkheden of vaardigheden hebben, is de ChristenUniewaarde veiligheid van belang. Bij deze burgers is er een vergrote kans dat misbruik wordt gemaakt van hun kwetsbaarheid. De overheid kan eraan bijdragen dat er veilige toegangen tot het internet en veilige digitale communicatiemiddelen worden aangeboden. De overheid kan ook bijdragen aan het vergroten van kennis over digitale gevaren door het geven van voorlichting.

Conclusie

Wanneer de overheid, bedrijven en organisaties gebruik maken van digitale technieken en middelen om informatie te verstrekken, te communiceren en diensten en producten aan te bieden, hebben zij een zekere verantwoordelijkheid om het mogelijk te maken dat iedereen die wil meedoen ook kan meedoen. Dat geldt in ieder geval wanneer het gebruik van digitale technieken en middelen noodzakelijk is om behoorlijk te kunnen meedoen aan de samenleving. ChristenUniepolitici moeten erop toezien dat de overheid haar eigen verantwoordelijkheid neemt om te waarborgen dat iedereen kan deelnemen aan de samenleving. Voor bedrijven en organisaties geldt dat bij het leveren van cruciale diensten, digitalisering niet in de weg mag staan. De ChristenUnie kan daarnaast stimuleren dat mensen op laagdrempelige wijze medemensen die digitaal minder vaardig zijn, kunnen helpen, zonder dat de digitaal minder vaardigen daarmee hun autonomie volledig uit handen moeten geven of makkelijk slachtoffer van misbruik worden.

3.3. Ruimte bieden aan publiek debat

Relevant voor: EP, EK, TK

Casus

Een groot techbedrijf⁸ biedt een dienst aan om korte berichten en plaatjes te delen. Steeds vaker zijn er mensen die via dit medium onwaarheden verkondigen. Het bedrijf worstelt met de vraag wat het ermee moet doen. Mag iedereen roepen wat hij of zij wil en is het bedrijf slechts een anoniem doorgeefluik? Of dienen pertinente onwaarheden te worden tegengesproken of uitgefilterd? Het bedrijf kiest voor het laatste, censuur. Op een gegeven moment worden ook berichten van politici voorzien van begeleidende tekst, of worden hun accounts zelfs tijdelijk geblokkeerd. Uiteindelijk besluit het bedrijf de president van het meest invloedrijke land in de wereld de toegang tot het platform te ontfagen. De rijkste man van de wereld is het daar echter niet mee eens. Hij koopt het bedrijf en geeft de voormalige president weer toegang tot de berichtendienst.

Afweging van waarden

De beginselverklaring van de ChristenUnie stelt dat we in een democratie worden uitgenodigd om vanuit onze waarden en overtuigingen mee vorm te geven aan de samenleving. De democratische samenleving bestaat bij de gratie van het publieke debat. Het maatschappelijk debat vindt plaats op verschillende plekken: in huiskamers, binnen scholen en universiteiten, verenigingen, kerken, bedrijven, maar ook via de media. Vanwege de beperkte ruimte die er is om meningen te verspreiden, filteren en selecteren traditionele media per definitie; de meeste doen dit naar eer en geweten,

⁸ Deze casus is gebaseerd op de ontwikkelingen rondom Twitter in de periode 2020 - 2023.

maar ook gestuurd door eigen aandachtsgebieden of interesses. Een pluriform medialandschap zorgt ervoor dat verschillende geluiden toch te horen zijn.

Met het ontstaan van online sociale media is er geen noodzaak meer om berichten te filteren. Ieder bericht kan gepubliceerd worden en heeft in potentie een wereldwijd bereik. Socialemediabedrijven hebben in eerste instantie de positie ingenomen dat ze niet verantwoordelijk zijn voor de informatie die via hun platform wordt verspreid. Dat standpunt is niet houdbaar. Waar overheden de taak hebben misdaden te bestraffen, hebben mediabedrijven de taak om de verspreiding van beledigingen, bedreigingen en illegale informatie tegen te gaan.

Sommige socialemediabedrijven gaan een stap verder in het tegengaan van de verspreiding van onjuiste of onwelgevallige informatie. Dat doen ze bijvoorbeeld door accounts op te schorten of bij een omstreden claim te verwijzen naar andere (feitelijke) informatie. Als het om een beperkt platform gaat, is dat niet problematisch. Maar wanneer commerciële socialemediakanalen zo groot zijn dat ze een belangrijk deel van de informatie-uitwisseling in de maatschappij verzorgen, heeft een inperking hiervan invloed op het publieke debat.

Ook heeft de overheid een rol om de vrijheid van vereniging te garanderen. Binnen de grenzen van de rechtsstaat hebben mensen het recht gemeenschappen en organisaties te vormen, waarin ze hun levensovertuiging delen. Ook op het internet kunnen platforms, fora en netwerken worden opgericht en gebruikt om (levens)overtuigingen te delen, ook wanneer die niet overeenkomen met de meerderheids-overtuiging, zolang ze maar blijven binnen de grenzen van de rechtsstaat – onder meer het verbod op discriminatie, belediging en bedreiging.

Een ander risico is dat socialemediabedrijven zelf gaan proberen om maatschappelijke opinies te beïnvloeden. Dit risico is groter bij platforms die in handen zijn van bedrijven in landen met minder democratische regimes. Beïnvloeding betekent een potentiële aantasting van onze vrijheid en ons democratisch bestel.

Conclusie

De overheid moet zorgen dat er voldoende ruimte blijft om het maatschappelijk debat in vrijheid en vanuit eigen overtuigingen te voeren, binnen bestaande wettelijke kaders. Op dit moment is er een aantal zeer grote commerciële socialmediabedrijven dat de facto een monopoliepositie heeft bij de verspreiding van informatie binnen bepaalde delen van de samenleving. De eigenhandige filtering van informatieverbreiding door deze bedrijven is een inperking van het publieke debat. De oplossing ligt in het doorbreken van deze monopolies, vooral op Europees en internationaal niveau, waar wetgeving zoals DSA (Digital Services Act) ook al gehandhaafd wordt. Net zoals de overheid de randvoorwaarden schept voor een pluriform mediabestel, zou de overheid ook randvoorwaarden moeten scheppen voor een pluriform online mediabestel: daarin mogen partijen niet te dominant worden, en moet ruimte zijn voor verschillende gemeenschappen die zich mogen organiseren via hun eigen principes.

De geplande EU Digital Markets Act, waarin grote spelers zijn aangewezen als poortwachter met extra verantwoordelijkheden, is een eerste stap in deze richting.

Tegelijkertijd ligt er nog steeds veel verantwoordelijkheid bij private commerciële bedrijven. Een echt decentrale oplossing lijkt daarom wenselijker om de monopoliepositie van socialemediareuzen en hun greep op het publieke debat te doorbreken, maar is vanuit de huidige situatie moeilijk te organiseren. Het decentrale socialemediaplatform Mastodon (<https://joinmastodon.org/nl-NL>) is een mooi voorbeeld van de manier waarop dat technisch vormgegeven kan worden.

3.4. Polarisation en veiligheid

Relevant voor: EP, EK, TK

Casus

Een kerkdienst met als thema 'Het Bijbelse huwelijk' wordt, zoals gebruikelijk, uitgezonden op het eigen kerkkanaal van YouTube. Een paar minuten van deze dienst, over het huwelijk van man en vrouw, worden ook gedeeld op andere kanalen, met afkeurende opmerkingen ernaast. Binnen enkele dagen zijn er sterk afwijzende reacties op deze video en de voorganger krijgt te maken met doxing: zijn woonadres en telefoonnummer worden gedeeld in de reacties, waardoor hij zich genoodzaakt voelt tijdelijk ergens anders te verblijven en zijn telefoonnummer te veranderen. Het socialemediabedrijf dat de kanalen aanbiedt neemt wel maatregelen tegen het doxen, maar verwijdt niet de reacties van voor- en tegenstanders van de preek, met een verwijzing naar de vrijheid van meningsuiting. Er is een online petitie gestart om van YouTube te eisen het kanaal van de desbetreffende kerk van YouTube te verwijderen, in verband met 'belediging en aanzetten tot haat'.

Afweging van waarden

Vrijheid van vereniging en vrijheid van godsdienst – 'Binnen de grenzen van de rechtsstaat hebben mensen het recht gemeenschappen en organisaties te vormen, waarin een levensovertuigingsgedeelte wordt'. Ook op het internet kunnen platforms, fora en netwerken worden opgericht en gebruikt om (levens)overtuigingen te delen. Bij het delen van overtuigingen dienen de grenzen van de rechtsstaat – inclusief de strafbaarstellingen voor onder meer discriminatie, belediging en bedreiging – in acht te worden genomen.

Onpartijdigheid – 'De overheid is onpartijdig'. Voorkomen moet worden dat de overheid het uiten van haar onwelgevallige overtuigingen belemmert.

Weerbare democratie – 'De overheid verweert zich krachtig wanneer de vrijheid in ons land wordt bedreigd (...) In de strijd tegen onrecht en onvrijheid dienen we onszelf nooit te verlagen door zelf wapens van onrecht en onvrijheid te grijpen.'. Ook door digitale technieken kan de vrijheid worden bedreigd, bijvoorbeeld doordat het publieke debat onmogelijk wordt gemaakt door het verspreiden van leugens en desinformatie, door beledigingen en bedreigingen, of door het creëren van filterbubbels en echokamers. Ook hier geldt dat Europese wet- en regelgeving (zoals de DSA) een grote rol mogen spelen in het reguleren van deze zaken.

Conclusie

De overheid moet balanceren tussen het garanderen van de vrijheid van vereniging en van het delen van levensovertuigingen, en het krachtig verweren tegen bedreigingen van die vrijheid. Het verweer mag zelf geen onvrijheid opleveren: dus geen censuur. De grenzen zijn de grenzen van de rechtsstaat: de Grondwet en andere wetten. De overheid moet enerzijds optreden tegen overtredingen van strafbepalingen en anderzijds de weerbaarheid van burgers vergroten door het stimuleren van onderwijs en een breed publiek debat. De overheid ziet erop toe dat de grenzen van de rechtsstaat ook op sociale media worden gehanteerd en ze verplicht bedrijven deze regels te handhaven. Er is geen recht om medemens te bedreigen of te smaden. De overheid grijpt in door misdaden op te sporen en te bestraffen. Er zullen betere mogelijkheden moeten worden ontwikkeld om de identiteit van online bedreigers te achterhalen. Preventie door online beledigingen en bedreigingen moeilijker te maken is ook nuttig (bijvoorbeeld door het verplichten van automatische herkenning van smaad en bedreiging). Doxing moet worden tegengegaan, evenals het 'live tracken' van personen. Privégegevens van iemand mogen niet geplaatst of gepubliceerd worden zonder iemands uitdrukkelijke toestemming. Ook elke bedreiging om privégegevens openbaar te maken of het aanzetten van anderen hiertoe is verboden, evenals het vragen of aanbieden van een premie in ruil voor het plaatsen van iemands privégegevens.

3.5. Cryptocurrency

Relevant voor: TK, EK, EP

Casus

Aleksandr heeft een nieuwe stichting opgericht om oorlogsslachtoffers uit Oekraïne te helpen. Nu nog een bankrekening openen, anders kun je helemaal niets. Maar wat nu? Alle grote banken komen met hetzelfde verhaal: vul een formulier van zestien kantjes in, dan beoordelen we dat en hoort u over zes weken of u uitgenodigd wordt voor een gesprek om te kijken of u een bankrekening kunt krijgen. Het schijnt te maken te hebben met uit het buitenland ontvangen giften zonder dat daar een prestatie tegenover staat, en angst bij banken voor witwassen. Wat nu? Gelukkig is er een alternatief! De digitale munt van Facebooks moederbedrijf Meta is dan weliswaar niet doorgegaan, maar gelukkig hebben we de Bitcoin nog. [Zes maanden later:] Ai, de keuze voor crypto is niet goed uitgepakt. FTX, tot voor kort een van de meest gerenommeerde namen in de cryptowereld, vroeg in een wolk van fraude het faillissement aan. De beurs had naar schatting een miljoen klanten. Door het debacle hebben ook veel andere investeerders het vertrouwen in cryptovaluta verloren, waardoor de hele markt klappen krijgt. Aleksandr's geworven giften zijn verdampt....

Afweging van waarden

Cryptomunten bieden keuzevrijheid omdat ze de positie van banken doorbreken. Ze dragen daarmee ook bij aan het begrenzen van de macht van de (commerciële) banken: er is een alternatief voor het systeem van banken. Onder de (meeste) cryptomunten ligt blockchain als technologie. Daarmee kan anonimiteit worden gegarandeerd.

Ieder voordeel heeft in dit geval echter zijn nadeel. De cryptocurrencymarkt onttrekt zich aan het gezag van de overheid en wil zich niet laten ordenen en begrenzen. Een wereldwijde markt waarin veel geld omgaat en waarmee een publiek belang gemoeid is, dient geordend en begrensd te worden en dat vraagt om samenwerking tussen overheden wereldwijd. Bij crypto's bestaat er niet iets als een entiteit die aansprakelijk is, wat betekent dat vorderingen niet afdwingbaar zijn. Het feit dat er geen toezicht is, en er ook geen garanties zijn op dekking van een belegging in cryptomunten maakt crypto tot een soort 'gokspel' met kenmerken van een piramidespel. Van het eerste is de ChristenUnie principieel tegenstander, het tweede is wettelijk verboden.

De anonimiteit van cryptocurrencies zijn ook niet altijd even dienstbaar aan de samenleving. Ze biedt vooral mogelijkheden om misbruik te maken van kwetsbaren en om geld dat is verdiend met misdrijven weg te sluizen en wit te wassen.

Als neveneffect dient genoemd te worden dat het stroomgebruik voor minen van cryptocurrencies (met name Bitcoin) jaarlijks even hoog is als dat van middelgrote westerse landen.

De crash van cryptobeurs FTX moet beleidsmakers aan het denken zetten. Maar dit hoeft niet per se te leiden tot een verbod. Cryptomunten hebben, ondanks de problemen, nog steeds de potentie om efficiëntie en transparantie in financiële systemen te vergroten. De crash van FTX heeft wel aangetoond dat het tijd is dat de politiek begint met het reguleren van de cryptomarkt.

Conclusie

Idealiter wordt een cryptomunt door een centrale bank gegarandeerd en op maat van de burgers ontworpen: gedekt, met respect voor de privacy en aandacht voor gegevensbescherming. Cryptomunten in de huidige vorm hebben deze garanties niet. Dat roept vragen op over hun toegevoegde waarde. De cryptomarkt zal zich op zijn minst onder het gezag van de overheid (bijvoorbeeld in Europees verband) moeten stellen die regels kan opstellen voor het maken (minen) en verhandelen van de crypto's. Als dit

niet mogelijk is, lijken cryptomunten vooral een ongereguleerd beleggingsfonds. Vanuit ChristenUnie-waarden kun je deze praktijk afkeuren en in de huidige vorm zelfs verbieden.

3.6. Online onderwijs

Relevant voor: EK, TK.

Casus

De klas is stil, alle kinderen zijn aan het rekenen. Op hun iPad hebben ze snelrekenen. Dit is voor juf Indra een mooi moment om de leerresultaten van de leerlingen te bekijken. Ze gaat naar de online leeromgeving waarin alle digitale gegevens van de leerlingen staan. Zo kan ze snel de slagingspercentages en de vorderingen van de kinderen zien. Met deze gegevens gaat ze het persoonlijk leerplan van haar leerlingen aanpassen zodat elk kind de juiste lesstof krijgt. Dit is niet alleen handig voor Indra, de ouders van de leerlingen zijn ook blij als hun kind de aandacht krijgt die het verdient.

Afweging van waarden

Digitalisering in het onderwijs brengt voordelen met zich mee. De leergegevens van kinderen zijn snel en makkelijk terug te vinden. Leerlingen die tijdelijk niet naar school kunnen omdat ze bijvoorbeeld in het ziekenhuis zijn, kunnen online les volgen. Studenten volgen hun hoorcolleges op afstand, wat prettig is als ze ver van hun onderwijsinstelling wonen. Tijdens de coronapandemie kon het onderwijs doorgaan op afstand, zij het met beperkingen.

Tegelijkertijd zijn er ook ontwikkelingen waar kanttekeningen bij te plaatsen zijn. De ChristenUnie staat voor een samenleving waarin mensen elkaar fysiek ontmoeten en waarin mensen hun relaties fysiek kunnen onderhouden. Het onderwijs gaat niet alleen om het opdoen van kennis, het is juist een plek waar sociale relaties centraal staan. Daarom is het belangrijk dat scholen, zowel in het primair als het middelbaar en vervolgonderwijs, fysieke ontmoetingsplekken blijven. Digitaal onderwijs heeft voordelen in bepaalde omstandigheden, maar het is geen directe vervanger voor het sociale aspect binnen het onderwijs.

Daarnaast is het belangrijk om na te denken over de begrenzing van het delen van data van leerlingen en studenten. Op dit moment werken veel leerlingen op gratis of goedkope soft- en hardware. Denk bijvoorbeeld aan laptops met Googlesoftware die scholen van Google krijgen. Hierdoor krijgt Google data over de leerlingen. Deze data, verkregen in het publieke domein, verdwijnen dus achter de gesloten deuren van een commerciële organisatie.

Conclusie

Het onderwijs is en blijft een plek waar leerlingen en studenten praktische, theoretische én sociale kennis opdoen. Daarom is het belangrijk dat leerlingen en studenten elkaar en hun leraren fysiek blijven ontmoeten. Online onderwijs is in bepaalde omstandigheden handig of zelfs noodzakelijk (zoals tijdens de coronapandemie), maar het is geen vervanger voor fysiek onderwijs. Daarnaast is het belangrijk dat er binnen het onderwijs meer aandacht gaat naar de begrenzing van data-uitwisseling met commerciële organisaties. Het leslokaal is van het onderwijs en het is geen plaats waar data, anders dan voor onderwijsdoelen, verzameld moeten worden, laat staan dat deze data automatisch toevallen aan commerciële bedrijven.

3.7. Algoritmische besluitvorming

Relevant voor: EP, EK, TKEP, EK, TK, PS, WS, GR

Casus

Judith en Ivano hebben na een lange tijd eindelijk succes met hun zoektocht naar een woning. Hun bod is zowaar geaccepteerd! De gekte op de huizenmarkt, met biedingen ver boven de vraagprijs, is

een beetje tot bedaren gekomen. Het stel heeft goed nagedacht welk bedrag per maand ze kunnen besteden aan woonlasten en heeft op basis van online rekentools een goede inschatting gemaakt van hun budget. Hun bieding past daarin. Nu naar de bank! In hun online dossier geven ze alle informatie die gevraagd wordt: persoonsgegevens, werkgeschiedenis, inkomen, schulden, enzovoort. Na een week ontvangen ze een mail dat de bank de hypotheek niet kan verstrekken omdat het risico te hoog is. Ze bellen naar de bank om een toelichting. Helaas horen ze weinig meer details. 'Uit de analyse is gebleken dat het risicoprofiel voor deze financiering te hoog is.' Ze vragen zich af waar het mee te maken heeft. Is het de combinatie van de studieschuld van Judith en haar creatieve beroep met fluctuerend inkomen? Of heeft het met Ivano's Italiaanse paspoort te maken? Of met de wijk waarin hun nieuwe huis staat? Met hulp van een kleine onderhandse lening van Ivano's familie lukt het ze toch nog om het huis met een iets lagere hypotheek te kopen.

Afweging van waarden

Dat computers worden gebruikt om gegevens te ordenen, te structureren en te selecteren is onvermijdelijk. Wanneer algoritmes voor het nemen van besluiten worden ingezet door overheidsorganisaties of bedrijven spelen minimaal twee vragen een rol: 1) zijn de beslissingen eerlijk? en 2) wie is er verantwoordelijk?

In onze Grondwet, en ook in de ChristenUniebeginselverklaring, is gelijkheid een belangrijke waarde. Iedere burger is gelijk voor de wet. In de bijlage wordt uitgelegd dat een bias (ingeslopen vooroordelen in algoritmes) niet is uit te sluiten en zelfs moeilijk te herkennen. Hierdoor kan ongelijke behandeling optreden, en alleen al om deze reden is grote voorzichtigheid geboden bij de toepassing van algoritmes voor het nemen van besluiten. Een andere relevante ChristenUniewaarde is de zorg voor kwetsbaren. De overheid dient een schild te zijn voor de zwakken. Voorbeelden uit het verleden, bijvoorbeeld de toeslagenaffaire en SyRI, laten zien dat vaak kwetsbare groepen zijn benadeeld door algoritmische besluiten. Extra voorzichtigheid is dus geboden. Een belangrijke rol van de overheid is volgens de beginselverklaring van de ChristenUnie het beschermen en handhaven van het recht. Dit betekent ook dat de overheid regels moet opstellen voor het gebruik van modellen. Er dienen waarborgen te zijn om te voorkomen dat gebrekkige modellen worden gebruikt. Dat kan bijvoorbeeld door een openbaar algoritmeregister in te richten, waarin organisaties verantwoording moeten afleggen over de manier waarop data verzameld zijn en over de kwaliteitstoetsen die zijn uitgevoerd om vooroordelen en discriminatie te voorkomen. Deze eis kan op gespannen voet staan met commerciële bedrijfsbelangen. Bedrijven willen immers hun specifieke methoden het liefst geheimhouden.⁹ In dit geval weegt het belang van gelijke behandeling zwaarder. Verschillende gemeenten experimenteren reeds met registers. Regelgeving rondom dit onderwerp is volop in ontwikkeling en ook de Europese AI-Act bevat elementen die hieraan kunnen bijdragen.

Een specifiek risico bij het gebruik van AI-modellen is dat ze voorspellen op basis van afgeleide in plaats van directe kenmerken (correlatie versus causaal verband). Een klassiek voorbeeld is een model dat geleerd heeft dat mensen met een bepaalde postcode een groter risico lopen om fraude te plegen. Er is uiteraard geen causaal verband tussen het wonen in een wijk en het plegen van fraude, maar er kan een correlatie zijn doordat er bijvoorbeeld in die wijk een groter aantal mensen dan gemiddeld werken in een sector die meer fraudegevoelig is. Het is van belang om te voorkomen dat dit soort indirecte factoren een rol spelen bij voorspellingen die mensen betreffen.

Een belangrijke ChristenUniewaarde is dienstbare macht, de notie dat macht dienstbaar moet zijn aan het recht. Deze waarde gaat uit van menselijke verantwoordelijkheid. Machines kunnen geen verantwoordelijkheid nemen. Het is daarom van belang dat er altijd een mens verantwoordelijk is en blijft voor geautomatiseerde besluiten en gedragingen van computers en machines, en dat die persoon aansprakelijk is voor de gevolgen.

⁹ Het is de vraag of een register daadwerkelijk de concurrentiepositie van een bedrijf ondergraaft. Het is vaak nog heel ingewikkeld om op basis van informatie over data, en methoden en toegaste controles een vergelijkbaar systeem te ontwikkelen.

Volgens het uitgangspunt dat in een democratische rechtsstaat overheidsmacht wordt begrensd door het recht en door verantwoording, moeten beslissingen altijd verantwoord kunnen worden. Dit impliceert dat besluitvorming transparant moet zijn: het moet duidelijk zijn op basis van welke criteria en afwegingen een keuze tot stand is gekomen. Met de huidige stand van de techniek zijn veel AI-algoritmes niet uitlegbaar: het is niet duidelijk op welke grond conclusies worden getrokken. Dit vormt dit een principiële beperking voor de toepassing van algoritmes door de overheid. Bedrijven hebben hier wellicht wat meer ruimte, omdat er vaak een alternatief is voor het gebruik van diensten van een bedrijf. Hoe essentiëler de dienstverlening voor de maatschappij (denk bijvoorbeeld aan energiebedrijven), hoe kleiner deze ruimte wordt.

Conclusie

Ondanks de soms hoge kwaliteit van de voorspellingen van AI-modellen, zouden overheidsbeslissingen nooit alleen hierop mogen worden gebaseerd, omdat dit in tegenspraak is met het principe dat overheid zelf aanspreekbaar is op gemaakte keuzes. Het kan wel nuttig zijn om deze technieken in te zetten om beslissingen voor te bereiden, mits de uiteindelijke beslissing zelf objectief beargumenteerd wordt. Voor bedrijven is er iets meer ruimte voor de toepassing van algoritmische besluitvorming, maar de overheid dient eisen te stellen aan de kwaliteit van door haar gebruikte besluitvormende algoritmes en dient informatie te verstrekken over haar gebruik van automatisch gegenereerde algoritmes, bijvoorbeeld door een algoritmeregister.

Een praktisch aspect van de communicatie over algoritmische besluitvorming is dat de overheid ook bereikbaar moet zijn voor uitleg van gemaakte keuzes. Gemeenten, provincies, de rijksoverheid en de overheidsdiensten zullen een telefonisch of fysiek loket moeten hebben waar burgers terecht kunnen die vragen hebben over een bepaald besluit, bijvoorbeeld het weigeren van een vergunning of de toekenning van een toelage. Computer says no mag geen eindpunt zijn. Voor uitleg en eventueel herziening van een besluit dient altijd intermenselijk contact mogelijk te zijn met ambtenaren die kennis van zaken hebben.

Om te voorkomen dat mensen benadeeld worden op grond van generieke kenmerken, moet de overheid eisen stellen aan de data waarmee modellen getraind worden. Bijvoorbeeld de eis dat modellen alleen getraind mogen worden op kenmerken die een causaal verband kunnen hebben met de voorspelde waarde.¹⁰ Zo zou een model dat voorspelt of iemand een goede basketballer wordt wel getraind mogen worden op de kenmerken lengte en leeftijd, maar niet op de kenmerken haarkleur of woonplaats. Deze voorwaarden kunnen gecontroleerd worden door transparantie te vereisen in een algoritme-register.

3.8. Autonome wapensystemen

Relevant voor: EP, EK, TK

Casus

China blijkt al jaren te bouwen aan autonome wapensystemen (LAWS), blijkt uit onderzoek van de VS. Terwijl vredesorganisaties, het Rode Kruis en onderzoekers oproepen tot een verdrag dat deze wapens deels reguleert en deels verbiedt, stellen de VS en Turkije voor om in NAVO-verband ook LAWS te gaan ontwikkelen om preventief een afschrikwekkend tegenwicht te bieden aan de groeiende militaire macht van China.

Afweging van waarden

Macht draait om verantwoordelijkheid nemen. We zijn geroepen macht dienstbaar te maken aan recht. De overheid dient verantwoording af te leggen over haar eigen handelen, ook waar het Defensie betreft.

¹⁰ Dit betekent niet dat bepaalde kenmerken (zoals bijvoorbeeld huidskleur of etniciteit) per definitie niet gebruikt mogen worden. In het geval van het voorspellen van een specifieke ziekte die bijvoorbeeld samenhangt met etniciteit, zou deze factor wel gebruikt mogen worden.

Overheidsbeslissingen mogen niet gebaseerd worden op zelflerende systemen, omdat deze systemen geen (geldige) verantwoordelijkheid kunnen nemen voor beslissingen. Daarmee wordt aan een belangrijke voorwaarde voor de rechtsstaat en de democratie niet voldaan, namelijk dat functionarissen uiteindelijk aansprakelijk zijn voor beslissingen. Daarbij speelt een rol dat bij beslissingen door zelflerende systemen, de uitkomsten per definitie of in de praktijk onnavolgbaar zijn. Deze overweging geldt des te dringender voor militair handelen, waarbij levens op het spel staan en in veel gevallen actief levens worden beëindigd. Autonome wapensystemen die het zelflerend vermogen hebben om steeds meer destructie te plegen, zijn potentieel onbegrensd in het aanleren van destructie.

We zijn geroepen het menselijk leven te beschermen. Het leger speelt een duidelijke rol bij het waarborgen van gerechtigheid en vrede in de samenleving en kan wapens gebruiken om gerechtigheid en vrede te handhaven. Een militair ingrijpen geldt als noodzakelijk kwaad, alleen na en tegelijk met doorgaande diplomatieke inspanningen, sancties en andere niet-militaire middelen om een terugkeer naar vrede te bewerken. Deze overwegingen gelden op macroniveau (beslissen tot oorlog), maar op vergelijkbare wijze ook op microniveau (beslissingen in oorlog): de militair die als mens besluit wel of niet dodelijk geweld in te zetten, kan niet worden vervangen door een autonoom opererend systeem. Volledig autonome wapensystemen zijn niet in staat om die afweging van het juiste middel op het juiste moment te maken.

Hoewel we technologische ontwikkelingen liever niet als wedstrijd benaderen, zien we deze dynamiek – om begrijpelijke redenen – wel terug in overwegingen om autonome wapensystemen te ontwikkelen: een wapenwedloop is per definitie een wedstrijd waarbij de al dan niet vermeende voorsprong van de ander de ontwikkeling van technieken drijft. Het gevaar is daarbij dat ethische overwegingen en vragen buiten beeld raken. Hoewel een goed ontwikkeld wapenarsenaal de kans op een militair conflict kan verkleinen, ligt een duurzame oplossing voor conflicten niet in het militaire maar in het politieke domein. In de discussie over zelflerende wapensystemen is het daarom goed om morele vragen voor diverse scenario's uit te diepen.

Conclusie

Volledig autonome, zelflerende wapensystemen kunnen weliswaar heel effectief zijn, maar de inzet van deze systemen is niet te rijmen met de verantwoordelijkheid die de overheid heeft voor haar handelen. Het gebruik van dodelijke wapens is een zware verantwoordelijkheid en vereist daarom de betrokkenheid van menselijk handelen.

3.9. Digitale identificatieplicht

Relevant voor: EP, EK, TK

Casus

Kim is dol op Disneyfilms. Daarom praat ze vaak mee met discussies op een Disneyforum. Dat doet ze onder een pseudoniem. Haar collega's bij de gemeente hoeven niet per se achter haar hobby te komen als ze haar naam googelen. Ook haar kinderen zijn dol op de Disneyfiguren. Voor de verjaardag van haar zoontje wil ze een verzameling Disneypoppetjes kopen. Op Marktplaats heeft ze een mooie verzameling gezien. In de winkel kosten ze wel honderd euro en hier maar vijftig. Ze maakt een afspraak met de verkoper met de naam 'Disneypop' en betaalt alvast het afgesproken bedrag. Als ze een paar dagen later de poppetjes nog niet heeft gekregen is het account verwijderd. Kim is opgelicht.

Afweging van waarden

Bij digitale communicatie – via het internet, sociale media of berichtenapplicaties – is anonimiteit het uitgangspunt. Het achterhalen van een persoon achter een gebruikersnaam is moeilijk. Het is niet onmogelijk, maar het kost wel veel tijd en het heeft niet altijd resultaat. Anonimiteit heeft zijn voordelen.

Zo kun je aanwezig zijn op het internet zonder dat dit sporen nalaat die gelijk naar jouw persoon verwijzen. Anonimiteit heeft ook nadelen. Anonieme personen kunnen eenvoudig en vaak ongestraft andere personen beledigen, bedreigen of oplichten.

Vanuit ChristenUniewaarden kan enerzijds worden gewezen op het belang van een persoonlijke levenssfeer. Andere mensen – en bedrijven en de overheid al helemaal – gaat het in principe niet aan, wat iemand binnen de digitale ruimte doet. Anderzijds maakt de anonimiteit het ook gemakkelijk om onrecht te doen en (kwetsbare) medemensen te beschadigen. De overheid heeft als taak het recht te beschermen en te handhaven, maar dit is lastig als de kwaaddoeners zich kunnen verschuilen achter bijnamen.

Een mogelijke oplossing is een digitale identificatieplicht. Hierbij kan een parallel worden getrokken met de fysieke wereld. Net zoals van burgers in de fysieke publieke ruimte wordt verwacht dat zij zich kunnen identificeren als hierom wordt gevraagd, zou dat ook in de digitale fysieke ruimte moeten kunnen. In de fysieke ruimte is een identificatieplicht niet absoluut, maar beperkt tot de gevallen waarin aan wettelijke voorwaarden wordt voldaan. Een vergelijkbare regeling kan worden uitgewerkt voor digitale identificatie. Het gaat dan om een verplichting tot identificatie als dit in het belang is van de openbare (digitale) veiligheid of als er een redelijk vermoeden is dat er iets strafbaars is gebeurd. Denk aan identificatie bij bedreigingen op sociale media of oplichting via Marktplaats. Een digitale identificatieplicht is daarmee niet hetzelfde als altijd herkenbaar moeten zijn op het internet. Relatieve anonimiteit blijft het uitgangspunt, net zoals dat het geval is in de fysieke wereld. Technisch zal de identificatieplicht zo moeten worden vormgegeven dat met terugwerkende kracht een identiteit kan worden opgevraagd, zonder dat daardoor alle digitale bewegingen van burgers worden opgeslagen in een gegevensbank. Bij het vormgeven van een digitaal identiteitsbewijs moet worden voorkomen dat deze makkelijk kan worden gestolen of gekopieerd. Identiteitsfraude draagt immers niet bij aan een veilige digitale wereld.

Een digitale identificatieplicht is niet hetzelfde als het creëren van een digitale identiteit (in het Engels: e-identity) die overheden en bedrijven kunnen gebruiken om overheids- of bedrijfsdiensten aan te bieden. Bij een digitale identiteit bestaat al snel het gevaar dat alle digitale gegevens die over een bepaalde persoon beschikbaar zijn, worden verzameld en met elkaar verbonden. Dit nodigt uit tot het opstellen van profielen, met alle gevaren die daarbij horen, zoals een verregaande inmenging in het persoonlijke leven van burgers door de overheid of door bedrijven. Het past bij de ChristenUnie om de macht van grote bedrijven en de macht van de overheid te willen begrenzen. De angst voor een te grote inmenging van bedrijven of de overheid in het leven van burgers mag er echter niet toe leiden dat de overheid niet het gereedschap krijgt dat zij nodig heeft in haar opdracht de ordening van de samenleving te bewaren. Daar komt bij dat absolute anonimiteit zich moeilijk verhoudt tot de verbondenheid die mensen in een samenleving behoren te hebben. Onderdeel zijn van de samenleving betekent dat we elkaar tot verantwoording kunnen roepen – en dat lukt alleen als iemands identiteit bekend is.

Conclusie

Net als in de fysieke ruimte is in de digitale ruimte relatieve anonimiteit het uitgangspunt. Evenmin als iedereen hoeft te weten dat je op de fysieke rommelmarkt loopt, hoeft iedereen te weten dat je op de digitale Marktplaats shopt. Net als in de fysieke ruimte moet het in de digitale ruimte wel mogelijk zijn om, indien nodig, iemands identiteit vast te stellen. Bij het vormgeven van een digitaal paspoort moet worden voorkomen dat de data centraal worden verzameld en beheerd – of dat nu door een bedrijf of een overheid gebeurt.

3.10. Digitaal paspoort of e-identity

Relevant voor: EP, EK, TK

Casus

We maakten als samenleving kennis met digitale identificatie door het coronapaspoort: wat begon als een handige tool om bij te houden hoe vaak je een vaccin gekregen had, werd langzaam een middel om delen van de samenleving in grote mate te reguleren. Ook buiten de context van de pandemie wordt nagedacht over online identificatiemiddelen.

Afweging van waarden

Een paspoort is een gecertificeerd document dat dient om je te identificeren. In het paspoort zijn bepaalde kenmerken van je vastgelegd op basis waarvan je bepaalde rechten kunt uitoefenen. Met een paspoort kun je bijvoorbeeld bij een autoverhuurder identificeren zodat de verhuurder weet dat je je niet voordoe als iemand anders, en met het kenmerk 'Nederlandse nationaliteit' mag je vrij reizen in Europa. Online is steeds meer behoefte aan vormen van identificatie en het vastleggen van kenmerken waarmee je rechten kunt uitoefenen.¹¹ Het digitale aspect brengt echter ook een aantal (graduele) verschillen met zich mee. Zo is het heel gemakkelijk om functies toe te voegen, omdat het niet vereist is dat iedereen terugkomt op het gemeentehuis om een nieuwe versie op te halen. En doordat het automatisch te lezen is, is het veel gemakkelijker om een volledig betrouwbare controle toe te passen dan met papieren documenten.

De coronapas (de QR-code) die in 2021 in Nederland werd ingevoerd, is een specifiek voorbeeld van een digitale identiteit. Deze pas – in de vorm van een app – informeerde over vaccinaties van de eigenaar, een recente negatieve testuitslag en eerder herstel van corona. Op basis van deze informatie kon de eigenaar laten zien dat één van deze drie situaties voor hem of haar van toepassing was; specifieke informatie werd gedeeld. De overheid heeft de coronapas ingevoerd om na de lockdown vanwege de coronapandemie meer interactie in de samenleving toe te staan. Maar met de invoering daarvan werd de facto ook een deel van samenleving gesloten voor mensen die het bewijs niet konden (of wilden) laten zien. Het is daarom goed, onderscheid te maken tussen de functie van het vastleggen van kenmerken in een digitaal paspoort en de rechten die je op basis daarvan wel of niet hebt.

Vaak wordt gezegd dat digitale identificatiemethodes het risico met zich meebrengen op het aantasten van de privacy. Dat kan inderdaad het geval zijn, als wordt bijgehouden wie waar inlogt en wie wanneer op welke plek is. Technisch gezien hoeft dat echter niet per definitie zo te zijn en kan een e-identity ook beperktere informatie geven dan een paspoort dat veel gegevens bevat. In het geval van de coronapas is – mede dankzij een stevige lobby van wetenschappers en privacy-ambassadeurs – gekozen voor een opzet waarbij geen persoonlijke gegevens werden gedeeld, behalve de coronacriteria: vaccinatie, negatieve test of herstel.

Een andere relevante waarde is vrijheid. Volgens de ChristenUniegrondslag hebben mensen de vrijheid gekregen om vanuit hun diepste geloof en overtuigingen keuzes te maken in het leven. Een digitale identiteit maakt de drempel laag om specifieke voorwaarden te stellen aan het gebruik van bepaalde diensten of het bezoeken van bepaalde plekken, en deze voorwaarden ook honderd procent te handhaven. Dat kan een grote inperking betekenen van de vrijheid.

In het geval van de coronapas was het dit aspect dat de meeste maatschappelijke weerstand opriep. Waar de pas eerst alleen in een aantal specifieke situaties vereist was, werd de pas na verloop van tijd

¹¹ zie voor een nadere beschouwing over het verschil tussen een paspoort en een digitale identiteit: J. Boersma, *Je identiteit is geen paspoort* (2022).

vereist voor heel veel alledaagse plekken. De geleidelijke uitbreiding van het gebruik is een reëel risico¹² dat vraagt om een permanente afweging van waarden.

Specifiek voor de coronapas geldt dat er nog een andere waarde meespeelt, namelijk die van de 'ethiek van het leven', waarmee de ChristenUnie uitspreekt dat we geroepen zijn het menselijk leven te beschermen. Het coronatoegangsbewijs is primair ingevoerd als één van de maatregelen om de verspreiding te beperken van een virus dat vooral voor oudere en kwetsbare mensen dodelijk kan zijn. Daarmee droeg het bij aan de bescherming van het leven. In de afweging of een coronapas gerechtvaardigd is, zal deze waarde moeten worden afgewogen tegen de andere bovengenoemde waarden.

Een digitale identiteit kan zowel op nationaal als Europees (en zelfs wereldwijd) niveau worden ontwikkeld. Een voordeel van een Europese identiteit is dat ze grensoverschrijdende activiteiten makkelijker kan maken, bijvoorbeeld het huren van een auto in een buitenland. Tegelijk moeten we constateren dat een e-identity vaak gebruikt wordt voor interactie met de overheid en dat inwoners niet vaak met buitenlandse overheden te maken hebben. Een risico van een bovenationale digitale identiteit is dat er een compromis met andere landen moet worden bereikt over de functie en technische implementatie. Dit kan zorgen voor een vorm die niet goed aansluit bij de nationale waardenafweging. Ook bij de coronapas was dit het geval: waar in de Nederlandse QR-code geen persoonlijke informatie stond, werden naam, geboortedatum en type vaccinatie wel verwerkt in het internationale coronareisbewijs. Een andere – betere – optie dan een Europese digitale identiteit is een nationale identiteit die technisch uitwisselbaar is met die van andere landen. In Europa lijkt de ontwikkeling in deze richting te bewegen.

Conclusie

Een digitale identiteit is niet per definitie problematisch volgens de ChristenUniewaarden. De risico's liggen vooral in de manier waarop de overheid zo'n identiteit inzet. Voorkomen moet worden dat een digitale identiteit wordt gebruikt om data te verzamelen en te verhandelen. Hiervoor zijn technische oplossingen beschikbaar, bijvoorbeeld door een e-identity vorm te geven als gedistribueerd systeem waarbij mensen zelf controle blijven houden over de informatie en met wie die gedeeld wordt. Het is ook belangrijk om te voorkomen dat mensen uitgesloten worden van bepaalde diensten door teveel te leunen op een digitale identiteit. Bovendien zal de overheid vooraf duidelijk moeten definiëren wat het doel en de functie van een digitale identiteit is, op basis van een zorgvuldige waarden- en belangenafweging. Het is belangrijk dat de overheid de verleiding weerstaat om zonder nieuwe belangenafweging functionaliteit uit te breiden. Bij een bovenationale e-identity moet erover gewaakt worden dat de vormgeving in lijn is met de nationale belangenafweging. Op dit moment lijken er nog geen grote voordelen te zijn voor een Europese e-identity. Ook de inzet van een digitaal paspoort op basis van medische gegevens, zoals de coronapas, vergt een afweging van belangen: in welke mate draagt het bij aan de bescherming van kwetsbare levens en rechtvaardigt dit de inbreuk die wordt gemaakt op de vrijheid van burgers?

3.11. Regulering van datagebruik

Relevant voor: EP, EK, TK

Casus

Jeanets kleinkinderen willen Jeanet graag helpen om meer op de hoogte te blijven van hun wel en wee. 'Oma, als u een smartphone neemt met WhatsApp, kunnen we met elkaar berichten en foto's uitwisselen. En dan kunt u ook in de familie-app!'. Ze regelen een tweedehands telefoon voor hun oma. 'O ja, om de telefoon in te stellen heeft u ook een e-mailadres nodig. Maar dat kan heel goed via Gmail,

¹² Zie bijvoorbeeld de ontwikkeling van het Indiase project voor biometrische identificatie Aadhaar. Dat is begonnen als een dienst waarvoor je kon kiezen of je er gebruik van wilde maken, maar inmiddels is die zo verweven met verschillende diensten (zoals een bankrekening en mobiel telefoonabonnement) dat het gebruik nauwelijks meer vrijwillig te noemen is.

kost niks.' Na een half uurtje heeft oma een werkende telefoon met WhatsApp. In de maanden daarna raakt Jeanet enthousiast over de nieuwe vorm van contact. Ze is met veel meer mensen gaan appen. Een vriendin wijst haar op Facebook. Misschien nog wel leuker! Jeanet kijkt even rond op de site en al snel wordt haar gevraagd om haar naam en telefoonnummer in te voeren, samen met een wachtwoord. En wat leuk, ze kreeg direct berichtjes te zien van mensen die ze goed kende! Wat Jeanet niet weet, is dat twee grote bedrijven intussen een uitgebreid profiel van haar maken. Ze is geld waard geworden. Meta, het moederbedrijf van Facebook en WhatsApp, weet zowel met wie als hoe vaak ze via WhatsApp communiceert, hoe lang ze kijkt naar welke berichten op Facebook, en welke sites ze bezoekt vanuit Facebook of WhatsApp. Google weet waar ze haar telefoon mee naar toe neemt, met wie ze mailt en hoe vaak, welke woorden in die mail voorkomen, welke websites ze bezoekt en welke zoekopdrachten ze uitvoert. Beide bedrijven gebruiken deze informatie om adverteerders aan te kunnen bieden om gerichte advertenties te tonen. Ook verkopen ze deze informatie aan andere bedrijven, die de gegevens over oma Jeanet ook weer inzetten om gericht reclame te kunnen maken.

Afweging van waarden

Veel van wat we doen, laat een digitaal spoor achter. Door de verregaande digitalisering van de maatschappij worden betaaltransacties, OV-gebruik, autogebruik, online surf- en zoekgedrag, communicatie en vaak ook beweeggedrag bijgehouden en opgeslagen. Het verzamelen van allerlei informatie over het (online) gedrag van mensen staat overduidelijk haaks op de waarde van privacy, het recht dat mensen hebben op een persoonlijke levenssfeer. Temeer omdat een aantal grote bedrijven door hun omvang en breed scala aan diensten in staat is om veel van dit soort gegevens samen te voegen en met elkaar te combineren. Hoewel bedrijven vaak claimen deze informatie niet op individueel niveau te gebruiken, is er weinig zicht op hoe ze wel gebruikt wordt. Duidelijk is wel dat er een enorm verdienmodel zit achter het profileren van mensen op basis van verzamelde gegevens. Het gebruiken van gebruikers als basis voor handelswaar is ook niet in lijn met de waarde die de ChristenUnie toekent aan de mens. De mens is geschapen als kroon op de schepping en mag niet gereduceerd worden tot een commercieel dataprofiel.

Er is nog een ander aspect. De honger naar data van grote bedrijven staat op twee manieren op gespannen voet met de waarde van vrijheid. De ChristenUniebeginself verklaring zegt dat mensen de vrijheid hebben gekregen om vanuit hun diepste geloof en overtuigingen keuzes te maken in het leven. Grote techbedrijven proberen ten eerste die vrijheid doelbewust in te perken door je vast te houden in hun eigen 'eco-systeem', zodat ze zo veel mogelijk data van je kunnen verzamelen en maximaal van je kunnen profiteren als klant. Als je een Android telefoon hebt, ben je verplicht een Google-account te gebruiken. En als je een Google-account hebt, worden je foto's automatisch opgeslagen in een Google-cloud. Je kaarttoepassing is standaard Google Maps, en je surfgemak is maximaal wanneer je Google Chrome gebruikt. Ten tweede wordt de vrijheid ingeperkt doordat de profielen worden ingezet om gebruikers gericht informatie te geven die bijdraagt aan het langer gebruiken van hun systemen (door bijvoorbeeld filmpjes aan te bieden die passen bij interesses). In het slechtste geval kan dit doelbewust worden ingezet om opinies te beïnvloeden – tot in het stembokje. Dit risico is nog groter wanneer techbedrijven verbonden zijn met statelijke actoren, zeker wanneer die staten minder democratisch zijn dan de onze of anderszins andere waarden hanteren. In dat geval kan ook de nationale soevereiniteit in het geding komen. We willen niet dat onze inwoners doelbewust beïnvloed worden door buitenlandse mogelijkheden.

Ook de waarde van publieke gerechtigheid is in dit geval relevant. De overheid dient het kwetsbare en de kwetsbaren te beschermen. Juist jongeren zijn grootverbruikers van sociale media en lopen daarmee extra risico om ten prooi te vallen aan verslavende technieken en advertenties die het doel hebben om hen geld te laten uitgeven. Voor apps of digitale toepassingen gericht op jongeren is het daarom gerechtvaardigd dat de overheid extra scherpe regels stelt om dataverzameling en -gebruik te voorkomen.

Ook kan de overheid verslavende technieken verbieden, juist voor toepassingen die door kinderen of jongeren worden gebruikt.

De overheid heeft volgens de ChristenUnie een rol als marktmeester. Wanneer de markt de samenleving gaat domineren of als marktpartijen hun macht misbruiken, grijpt de overheid in. Een aantal grote techbedrijven is zeer dominant, waardoor misbruik van macht niet is uitgesloten. Er is dus voldoende reden voor de overheid om in deze markt in te grijpen.

Conclusie

De 'markt' voor techbedrijven is niet in evenwicht. Bovendien is misbruik van gegevens niet uit te sluiten en is het ook nog moeilijk dit misbruik te controleren. Het is daarom gerechtvaardigd dat de overheid ingrijpt. Dat kan op verschillende manieren. De overheid heeft al veel zinvolle spelregels geformuleerd, bijvoorbeeld in de door de EU ontwikkelde AVG. Veel grote bedrijven houden zich daar niet aan, denk bijvoorbeeld aan TikTok. Stevigere handhaving van deze regels is een essentiële stap. Gezien de schaal en het werkgebied van de bedrijven ligt het voor de hand deze handhaving op Europees niveau op te pakken. De EU Digital Markets Act is een grote stap vooruit op dit gebied. De nationale overheid kan druk opvoeren door overtreders een verbod op te leggen. Daarnaast is het noodzakelijk om meer inzicht te eisen in het gebruik en de verzameling van data door bedrijven (transparantie). Ook dit kan het beste op Europees niveau worden georganiseerd. De European Data Protection Board zou een stevigere rol moeten krijgen. Daarnaast zouden techbedrijven verplicht moeten worden om het in ieder geval makkelijk te maken om hun diensten open te stellen voor mensen die ook diensten elders afnemen, en andersom, het mogelijk te maken voor hun klanten een deel van de diensten bij andere bedrijven af te nemen. Dit vereist interoperabiliteit van diensten, bijvoorbeeld door gebruik te maken van open API's. Ten slotte zou de overheid toepassingen kunnen stimuleren waarvan de technische opzet minder risico met zich meebrengt voor het ontstaan van machtsconcentraties. Gedacht kan worden aan gedecentraliseerde systemen waarin niet één partij de zeggenschap heeft, maar waarin verschillende partijen een deel van het systeem beheren (bijvoorbeeld Mastodon als alternatief voor Twitter). Een ander voorbeeld zijn gedistribueerde systemen die zo zijn vormgegeven dat de data bij gebruikers blijven en gebruikers expliciet toestemming moeten geven om die te delen.

3.12. Bewaren en vernietigen van gegevens (datajubeljaar)

Relevant voor: EP, EK, TK, PS, WS, GR

Casus

Derk heeft tien jaar geleden meegedaan aan een online prijsvraag. Daarvoor moest hij zijn e-mailadres en telefoonnummer registreren op een website. Hij won niets. Maar sindsdien krijgt hij wel regelmatig e-mailberichten en telefoontjes van het bedrijf dat de prijsvraag organiseerde in een poging om producten te verkopen. Ook andere jeugdzonden blijven Derk achtervolgen. Wanneer hij zijn naam opzoekt op Google, is een van de eerste hits een artikel van de wijkkrant waarin hij als 15-jarige stoer vertelt over het afsteken van illegaal vuurwerk. Ook naar zijn enthousiaste liefdesbetuiging voor Ajax die Derk onder eigen naam op een forum zette, kijkt Derk als jarenlang tevreden inwoner van Utrecht met gemengde gevoelens.

Afweging van waarden

De ChristenUnie vindt dat de overheid de persoonlijke levenssfeer van burgers moet beschermen. Hoe langer persoonsgegevens van burgers worden bewaard – door de overheid, door bedrijven en organisaties – hoe groter de inbreuk die daarmee wordt gemaakt op de persoonlijke levenssfeer. Niet voor niets schrijft de AVG voor, dat gegevens tijdig moeten worden vernietigd.

Het vernietigen van gegevens is ook van belang bij het beschermen van de vrijheid van mensen. De

ChristenUnie vindt dat mensen de vrijheid hebben om vanuit hun diepste geloof en overtuigingen keuzes te maken in het leven. Het vastleggen van gegevens bindt mensen aan de keuzes die ze in het verleden hebben gemaakt. Hierdoor wordt de ruimte kleiner om in het heden vrije keuzes te maken. Hoe meer en hoe langer gegevens worden bewaard, hoe vaker mensen worden geconfronteerd met het verleden. Het belemmert de mogelijkheid om tot inkeer te komen, om nieuwe inzichten te ontwikkelen, om tot andere geloofs- en levensovertuigingen te komen. Zolang de gegevens op het internet blijven staan, blijft Derk Ajaxfan en de persoon die illegaal vuurwerk afsteekt – ook al is hij dat niet meer.

De ChristenUnie vindt het ook belangrijk dat mensen de mogelijkheid moeten hebben om zich te verenigen, of juist af te keren van de vereniging waartoe ze behoorden. Gegevens over een persoon kunnen worden verzameld, bij elkaar gevoegd en verwerkt tot een profiel. Het gebruik van profielen kan vervolgens allerlei consequenties hebben: van het ontvangen van bepaalde advertenties tot de weigering om een aangevraagde uitkering te verstrekken. Hun profiel kan mensen dus belemmeren om radicaal te breken met het verleden. De keuzes uit het verleden blijven bepalen hoe een persoon (online) wordt benaderd.

Er zijn legitieme redenen voor overheden, bedrijven en organisaties om gegevens te bewaren. Zo kan dat nodig zijn om de afgesproken diensten te blijven leveren. Een samenleving is er bovendien bij gebaat dat gegevens bewaard blijven, en dat er een archief wordt bijgehouden dat ook door komende generaties kan worden geraadpleegd. Lastiger is het als gegevens worden gebruikt om gedrag te voorspellen. Gedragingen uit het verleden zijn een goede indicatie voor gedragingen in de toekomst. Zo is een strafblad een bruikbaar middel voor de inschatting of iemand bepaalde werkzaamheden kan uitvoeren. Tegelijkertijd willen we niet dat een misstap uit het verleden iemands leven voor altijd blijft bepalen.

Het kan vervelend zijn om gegevens te moeten vernietigen. Het is minder efficiënt wanneer overheden, bedrijven of organisaties meerdere malen om dezelfde gegevens moeten vragen. Bovendien neemt de kwaliteit van voorspellingen af als er minder gegevens beschikbaar zijn. Efficiëntie en beheersingsmogelijkheden zouden echter niet doorslaggevend moeten zijn. De Bijbel leert dat er soms rust moeten worden gehouden – elke week een dag op de sabbat en elke vijftig jaar een heel jaar, het jubeljaar, dat in het teken staat van een schone lei. De samenleving gedijs bij rust en bij de mogelijkheid om zonder lasten uit het verleden opnieuw te beginnen.

Conclusie

In de AVG staat dat gegevens tijdig moeten worden vernietigd. De overheid moet hierin het goede voorbeeld geven en gegevens niet langer bewaren dan strikt noodzakelijk is. De overheid moet er ook op toezien dat bedrijven en organisaties gegevens tijdig vernietigen. Ook als dit betekent dat op zichzelf nuttige gegevens hiermee verloren gaan.

Nieuw aan digitale technieken is dat het onmogelijk is informatie te delen zonder dat dit wordt vastgelegd, terwijl er bij fysieke verbale en non-verbale communicatie vaak niet meer overblijft dan een herinnering. Om misbruik van digitale gegevens te voorkomen zou de overheid kunnen stimuleren dat er meer technische mogelijkheden ontwikkeld worden om digitaal gegevens te verstrekken die na verloop van een zekere tijd onleesbaar worden – zoals ook Snapchat beloofde met foto's – en te garanderen dat burgers van deze technologie gebruik kunnen maken als de ontvanger geen legitiem belang heeft bij het langer bewaren van deze gegevens.

3.13. Consequenties van digitalisering voor veiligheid

Relevant voor: EP, EK, TK, PS, WS, GR

Casus

Bereket wordt op dezelfde dag twee keer getroffen door misbruik van de mogelijkheden die het internet biedt. Het waterschap waar hij werkt wordt slachtoffer van een ransomware-aanval, waarbij software waarmee de sluizen worden bediend ontoegankelijk wordt gemaakt tenzij er losgeld wordt overgemaakt.¹³ Op hetzelfde moment ontvangt Bereket via WhatsApp een bericht van zijn neef die wat geld wil lenen. Dat is niet de eerste keer, dus Bereket maakt een bedrag over – gek genoeg wel naar een andere rekening dan normaal. Als Bereket zijn neef daarop nog even belt, blijkt die helemaal niet om geld te hebben gevraagd. Bereket is opgelicht. Hij doet aangifte van beide misdrijven, maar de politie geeft hem weinig hoop op een snelle berechting. De daders zitten waarschijnlijk in een land dat niet mee wil werken met Nederlandse opsporingsonderzoeken.

Afweging van waarden

Van de mogelijkheden die het internet biedt kan misbruik worden gemaakt. Zodra een digitaal apparaat is aangesloten op het internet, kan een kwaadwillend persoon proberen het apparaat of de gegevens die erop staan te gebruiken voor oneigenlijke doelen. Er zijn talloze voorbeelden denkbaar: van een computernetwerk dat niet toegankelijk is totdat er losgeld is betaald, tot op het internet aangesloten koelkasten die onderdeel worden van een botnet. Het misbruik kan tot grote gevaren leiden voor de veiligheid of de integriteit van de samenleving. Het kan gaan om fysieke gevaren, als bijvoorbeeld objecten als stoplichten, sluizen, bruggen of elektriciteitsnetwerken worden overgenomen.

Het kan ook gaan om maatschappelijke gevaren, zoals het platleggen van overheidswebsites of het saboteren van verkiezingen. En het kan gaan om overlast en schade voor burgers en bedrijven, doordat zij slachtoffer worden van digitale misdrijven als oplichting, afpersing, bedreiging en belediging.

De ChristenUnie vindt de bescherming van de veiligheid van haar burgers een kerntaak van de overheid. De overheid is geroepen onrecht te bestrijden, het gemeenschappelijk belang te bewaken en het kwetsbare en kwetsbaren te beschermen, ook op het internet. Dit is minder eenvoudig dan het op het eerste gezicht lijkt. De macht van een overheid is beperkt tot haar burgers en haar grondgebied. Het internet is echter een 'world wide web'. Bovendien is het mogelijk grotendeels anoniem gegevens op het internet te delen en te bewerken.

De taak om het recht te beschermen vraagt om een nieuwe doordenking van de verhouding tussen nationale (en Europese) soevereiniteit enerzijds en de digitale wereld anderzijds. De ChristenUnie vindt het niet wenselijk dat internationale samenwerking in het teken staat van concentratie van macht. De nationale soevereiniteit mag door de samenwerking niet te veel worden verzwakt. Vanuit dat oogpunt is een wereldwijd en onbegrensd internet niet vanzelfsprekend. Het bestrijden van onrecht vergt regels en handhaving van de regels. Op nationaal of Europees niveau. Hierbij kan een parallel worden getrokken met de fysieke wereld. Degene die fysiek de deuren van een winkel barricadeert totdat losgeld wordt betaald, kan worden gestraft voor afpersing. Dat zou ook moeten gelden voor afpersing op het internet.

Het bewaken van de veiligheid mag niet leiden tot overname van de digitale ruimte door de overheid. De overheid dient terughoudend te zijn en de verantwoordelijkheden van andere maatschappelijke verbanden niet over te nemen. Tegelijkertijd mag de overheid zich niet zo ver terugtrekken dat de digitale ruimte een bandeloze plek wordt waar het recht van de sterkste geldt. Die ruimte zal snel worden ingevuld door commerciële bedrijven en organisaties zonder veel scrupules. Wederom kan een vergelijking met de fysieke publieke ruimte helpen. Het stadsplein wordt beheerd en bewaakt door de overheid, en vervolgens kunnen burgers en ondernemers er gebruik van maken om te recreëren, te protesteren,

¹³ Rijksoverheid, Hack bij Waterschap kan voor serieuze dreiging zorgen (2021).

marktkramen op te zetten of terrasstoelen neer te zetten. De afstemming tussen al deze partijen wordt gefaciliteerd door de overheid, zonder dat zij over mag gaan tot grootschalige surveillance van wat er op het marktplein gaande is.

Conclusie

De overheid moet het recht handhaven in de digitale ruimte, en waarborgen dat er digitale openbare orde wordt gecreëerd waar burgers, bedrijven en organisaties de ruimte krijgen om samen te leven. Het handhaven van een digitale openbare orde impliceert de mogelijkheid om normen te stellen en te handhaven. Daarom moet worden nagedacht over het afgrenzen van delen van het internet. Voor de handhaving moeten voldoende handhavers beschikbaar zijn die voldoende bevoegdheden hebben. Het waarborgen van een digitale openbare orde impliceert ook dat de digitale ruimte niet wordt overgenomen door techbedrijven als Google, Facebook, Apple en Amazon. De overheid zal monopolies dus moeten doorbreken en grote aanbieders die meerdere digitale diensten aanbieden moeten opsplitsen. Daarmee is niet gezegd dat de overheid vervolgens deze diensten moet aanbieden. Het zal aan de samenleving moeten worden overgelaten welke bedrijven en organisaties de openliggende taken gaan oppakken. Het waarborgen van een digitale openbare orde vergt ook dat burgers worden beschermd tegen de eigen gemakzucht. Een neutrale digitale openbare ruimte met meerdere aanbieders van afzonderlijke diensten kan ertoe leiden dat burgers vaker moeten inloggen, meer wachtwoorden moeten aanmaken en onthouden en vaker gegevens moeten invullen. Dat is ongemakkelijk. Maar hiermee geeft de overheid wel invulling aan haar opdracht om de burgers de ruimte te bieden om verantwoord te handelen.

3.14. Omgaan met sociale media

Relevant voor: EP, EK, TK

Casus

Geert maakt zich zorgen over zijn kinderen. Zijn zoon is eindeloos bezig met Minecraft en trekt zich zodra hij thuiskomt terug op zijn kamer om met schoolvrienden verder te bouwen aan hun eigen wereld. Op de momenten dat hij wel beneden is, bekijkt hij Minecraftfilmpjes op zijn smartphone. De dochter van Geert zit urenlang in een hoekje op de bank filmpje na filmpje te bekijken. Om weer contact te maken met zijn kinderen spreekt Geert af dat er aan tafel geen smartphone mag worden gebruikt. Dat is ook voor hemzelf wennen, want Geert had de gewoonte ontwikkeld om telkens even op nu.nl te kijken voor het laatste nieuws. Tijdens de gezamenlijke maaltijd klaagt de dochter van Geert dat de voetbalclub heeft verboden om smartphones mee te nemen naar het veld. Daardoor kan ze geen filmpjes meer maken van haar hooghoudtrucs. Geert vindt het niet zo'n gekke maatregel. Hij had bij een training een paar maanden geleden gezien dat het scherm vaak interessanter werd gevonden dan wat er op het veld gebeurde.

Afweging van waarden

Sociale media – TikTok, WhatsApp, Instagram, Facebook, YouTube, Discord, Reddit – hebben een verregaande invloed op de samenleving. Vooral jongere generaties besteden veel tijd aan het via een smartphone delen en met name kennisnemen van foto's, filmpjes en tekstberichten. Een kenmerkend beeld van onze samenleving is dat er meerdere personen zwijsend naast elkaar zitten, allen verdiept in hun eigen scherm. Over de wenselijkheid van sociale media kan verschillend worden gedacht. De sociale media zijn een bron van informatie en vermaak en dragen bij aan het onderhouden van contacten. Er zijn echter ook aanwijzingen dat veelvuldig gebruik van sociale media een negatieve invloed heeft op de mentale gesteldheid van met name jongeren.¹⁴

¹⁴ B. Keles e.a., "A systematic review: the influence of social media on depression, anxiety and psychological distress in adolescents", *International Journal of Adolescence and Youth*, 25(1), 79-93.

Vooropgesteld kan worden dat de bedrijven die de sociale media aanbieden een eigen verantwoordelijkheid hebben voor de kwaliteit van hun producten. In een andere casus wordt aandacht besteed aan de verantwoordelijkheid voor de verzameling en verwerking van gegevens door technologiebedrijven. Erkend moet worden dat veel sociale media zo zijn vormgegeven dat mensen zo lang mogelijk gebruik hiervan willen maken. In de strijd tegen de knappe koppen van Silicon Valley staat een individu op achterstand. Daarom moeten we als samenleving bepalen welke ruimte we willen bieden aan sociale media in het algemeen, en specifieke platformen in het bijzonder.

Nieuwe technologieën als sociale media vragen om een reactie van de samenleving. In het onderlinge gesprek moeten we met elkaar bepalen wat we wel en niet willen. Dit gesprek loopt onvermijdelijk achter de feiten aan. Daarbij bestaat het risico dat de negatieve effecten zich al verwezenlijken voordat een adequate reactie is geformuleerd, zoals het geval is bij sociale media. Dit zou niet per definitie moeten leiden tot ingrijpen van de overheid. Pas als het maatschappelijke debat is gevoerd, kan de overheid bepalen wat de maatschappelijke consensus is over het gebruik van sociale media en welke regels er eventueel nodig zijn om deze maatschappelijke consensus vast te leggen.

Maatschappelijke verbanden als gezinnen, scholen, verenigingen en bedrijven hebben een eigen verantwoordelijkheid en een eigen ruimte in de omgang met sociale media. Binnen het gezin mag worden bepaald op welke momenten wel en niet op een smartphone mag worden gekeken. Scholen hebben de vrijheid om keuzes te maken over het toelaten van een smartphone in de klas. De voetbalvereniging mag eigen regels opstellen over het gebruik van smartphones en apps tijdens voetbaltrainingen en wedstrijden en over het delen via sociale media van informatie die andere verenigingsleden betreft. Dit kan leiden tot verschillen. Dat mag echter geen reden zijn voor de overheid om de verantwoordelijkheid van maatschappelijke verbanden over te nemen.

De omgang met sociale media vergt nieuwe vaardigheden en attitudes, vergt een nieuwe sociale etiquette. Het aanleren van deze vaardigheden is de verantwoordelijkheid van ouders en leerkrachten en van iedereen die invloed heeft op het gedrag van medeburgers. Dit vergt constante alertheid, juist van opvoeders en leraren. Nieuwe sociale media en nieuwe digitale technieken komen snel op en kunnen binnen een korte tijd grote invloed uitoefenen op de samenleving. Hierin kan de overheid wel een rol vervullen. Niet door de taak van opvoeders en leraren over te nemen, maar wel door hun middelen aan te reiken om invulling te geven aan hun eigen taak. Door middel van voorlichting kan worden gewezen op het belang van het maatschappelijke debat over de omgang met sociale media en de rol die opvoeders, leraren en anderen kunnen hebben op het aanleren van nieuwe vaardigheden.

Conclusie

De verantwoordelijkheid voor een goede reactie op en de omgang met sociale media ligt bij de samenleving als geheel. In het onderlinge gesprek moet worden uitgekristalliseerd wat wel en niet wordt geaccepteerd. Het maatschappelijke middenveld kan daarbij een voortrekkersrol vervullen, door zelf regels op te stellen over het gebruik van smartphones en sociale media in scholen, op voetbalvelden, in ziekenhuizen, in repetitielokalen. Dit kan leiden tot uiteenlopende regels, maar dat hoeft geen reden te zijn voor de overheid om in te grijpen. Integendeel, uiteenlopende regels kunnen het maatschappelijke debat stimuleren. De overheid rest een ondersteunende taak, met name door het voorlichten en toerusten van opvoeders en leraren. Het is verstandig om niet te snel te reageren op nieuwe sociale media en nieuwe digitale technieken.

3.15. Leefbare kernen

Casus

De krokussen komen uit de grond, de vogels fluiten en de zonnestralen warmen je handen weer. Het is voorjaar, een goede tijd om de tuin aan te pakken. Op woensdag bedenkt Julian dat hij op zaterdagmiddag in zijn tuin aan de slag wil, maar dat hij daarvoor nog een aantal spullen nodig heeft. Hij kan hiervoor naar het tuincentrum gaan, maar hij moet de rest van de week werken. Hij zou op zaterdagochtend kunnen gaan, maar dan zal het wel druk zijn. Hij kan zijn benodigdheden ook online bestellen. Wel zo makkelijk en wat hij achteraf niet gebruikt, kan hij makkelijk retourneren. Als hij alles nu gaat bestellen, is het vrijdag sowieso in huis.

Afweging van de waarden

Wij staan als ChristenUnie voor een wereld waarin mensen elkaar ontmoeten en relaties met elkaar aangaan. Hiervoor zijn levendige kernen en wijken nodig. Het praatje in de supermarkt, de toevallige ontmoeting bij de schoenenwinkel of het goede gesprek met een gemeentelid bij het gezamenlijk koffiedrinken na de kerkdienst. Op deze toegankelijke plekken ontmoeten we elkaar en blijven gemeenschappen in stand. Wanneer we meer online leven (online winkelen, digitaal ontmoeten) verdwijnt een aantal van die analoge ontmoetingen waarin we samenleven, sociale interactie hebben en contact maken met allerlei mensen.

Digitalisering en de inzet van automatische systemen in plaats van mensen vormen niet de enige factor in de afname van levendigheid van de openbare ruimte; ook het verdwijnen van publieke voorzieningen als buslijnen en bibliotheken draagt bij aan de verschraving. Aan de andere kant: leegstaande winkels kunnen worden vervangen voor andere gemeenschappelijke nutsvoorzieningen.

Conclusie

Het is goed om van genoeg te genieten en om de relationele banden in lokale gemeenschappen te versterken. Door digitalisering verandert de winkelstraat, maar dit is niet automatisch een negatieve ontwikkeling wanneer er op andere manier invulling gegeven wordt aan de ruimtes om elkaar bedoeld en onbedoeld tegen te komen. Lokaal kunnen ondernemers geholpen worden om de digitaliseringsslag te maken of om na te denken over hun plek in een veranderende winkelstraat. Als Julian (uit de casus) weet dat het lokale tuincentrum met de fiets aan thuisbezorging doet in dezelfde tijd als een landelijke partij, dan is de kans groot dat hij bij zijn lokale tuincentrum koopt. We zijn voor het behoud van levendige kernen waar mensen uit de lokale gemeenschap elkaar ontmoeten. De taak van de overheid is om vanuit planologisch oogpunt de analoge publieke ruimte te behouden. Tegelijkertijd ligt er een maatschappelijke verantwoordelijkheid om zelf te blijven investeren in ontmoetingen in de openbare ruimte door deze plekken te bezoeken en bijvoorbeeld niet alleen voor de zelfscankassa te kiezen.

Hoofdstuk 4. Politieke speerpunten

De digitalisering gaat sneller dan de regulering ervan. Met het benoemen van ChristenUnie-uitgangspunten voor digitalisering willen we een leidraad bieden voor het omgaan met toekomstige digitaliseringsvraagstukken. Op dit moment zijn er echter al meer dan genoeg digitaliseringsproblemen die om aandacht vragen. In dit hoofdstuk sluiten we daarom af met enkele stellig geformuleerde aanbevelingen waarmee de ChristenUnie op korte termijn aan de slag kan.

De overheid geeft de hoogste prioriteit aan het strikt handhaven van de bestaande regels rondom dataverzameling en privacy.

De 'markt' voor techbedrijven is niet in evenwicht, en bovendien is misbruik van gegevens niet uit te sluiten en ook nog moeilijk te controleren. Juist kwetsbare mensen zoals kinderen en jongeren lopen het risico gebruikt te worden als bron voor dataverzameling en op grond daarvan te worden beïnvloed. Het is daarom gerechtvaardigd voor de overheid om in te grijpen. De overheid heeft al veel zinvolle spelregels geformuleerd, bijvoorbeeld in de door de EU ontwikkelde AVG. Veel grote bedrijven houden zich daar niet aan, denk bijvoorbeeld aan TikTok. Als geopolitieke belangen een rol spelen is de urgentie nog hoger. Stevige handhaving van deze regels is een essentiële stap. Wanneer bedrijven zich niet aan regels houden, treedt de overheid streng op, bijvoorbeeld door uitsluiting van de Nederlandse markt.

Het leslokaal is van het onderwijs en geen plek waar data voor commerciële doelen worden verzameld.

Aanbieders van digitale diensten kunnen een grote invloed hebben op domeinen als zorg en onderwijs. Het leslokaal is van het onderwijs en het is geen plaats waar data, anders dan voor onderwijsdoelen, verzameld moeten worden, laat staan dat deze data automatisch toevallen aan commerciële bedrijven. Scholen moeten een vrije keuze hebben uit aanbieders. Commerciële dataverzameling wordt daarom verboden en scholen worden (wanneer nodig ook financieel) ondersteund bij het gebruik van alternatieve opensourcendiensten waarbij de data eigendom blijven van de scholen.

Een Sociaal-Maatschappelijke Impact Analyse wordt vereist bij de introductie van technologie met potentieel groot effect op de samenleving.

Net zoals bij grote infrastructurele projecten een milieueffectrapportage (MER) is vereist, moeten ook de effecten van nieuwe technologie goed doordacht worden. De overheid zorgt dat zij een Sociaal-Maatschappelijke Impact Analyse uitvoert voordat zij een technologische innovatie introduceert die in potentie een groot effect heeft op de samenleving (denk aan de invloed van ChatGPT). De overheid vraagt dat ook van andere aanbieders. In de analyse wordt rekenschap gegeven van te verwachten gevolgen op aspecten van brede welvaart (gezondheid, onderwijs, milieu en leefomgeving, sociale cohesie, persoonlijke ontplooiing en (on)veiligheid en effecten op mensen ergens anders en generaties na ons) en kwetsbare groepen (digitaal niet-vaardigen, mensen met een verstandelijke beperking, kinderen en jongeren). Vervolgens kan een maatschappelijk gesprek plaatsvinden over maatschappelijke kosten en baten van een toepassing.

Technologie- en mediawijsheid moet een prominente rol krijgen in het curriculum van het primair en middelbaar onderwijs.

Ook burgers hebben een verantwoordelijkheid voor goede omgang met digitale technologie. De overheid moet eraan bijdragen dat kinderen en jongeren voldoende kennis hebben om verantwoorde keuzes te maken. In het onderwijs moet daarom ruim aandacht zijn voor de werking van digitale (media) technologie en de mogelijke effecten daarvan voor waarheidsvinding, beïnvloeding, verslaving, mentale gezondheid, personalisatie etc. Ook ouders moeten geholpen worden om voldoende kennis te hebben om hun kinderen daarin te begeleiden. Deze ondersteuning kan wellicht geboden worden in samenwerking met consultatiebureaus en de jeugdgezondheidszorg GGD.

Personalisatie wordt alleen toegestaan als burgers daar expliciet mee instemmen (opt-in) en bedrijven de plicht hebben om volledige transparantie te bieden over de gebruikte personalisatiemechanismen.

De overheid dient burgers te beschermen tegen het misbruiken van personalisatietechnieken. Misbruik kan leiden tot een verlies aan autonomie en vrijheid en tot verkoking van opvattingen. Internetgebruikers dienen daarom zelf expliciet in te stemmen met het toepassen van personalisatietechnieken. De keuze moet eenvoudig te maken zijn en niet gestuurd (uitleg op B1-niveau en universele knoppen voor de ja/nee-opties). In alle gevallen moet het mogelijk zijn om zeer eenvoudig inzicht te krijgen in de criteria die geleid hebben tot personalisatie (waarom krijg ik deze advertentie?).

De overheid investeert in training en ondersteuning van mensen met mindere vaardigheden op digitaal gebied.

Overheden nemen hun verantwoordelijkheid om te waarborgen dat iedereen kan deelnemen aan de samenleving. Zij zorgen voor voldoende ondersteuning van mensen die digitaal minder vaardig zijn en zij financieren initiatieven van bijvoorbeeld bibliotheken en organisaties als Cybersoek om mensen te helpen. Daarbij waken zij ervoor dat de digitaal minder vaardigen daarmee hun autonomie volledig uit handen moeten geven of makkelijk slachtoffer van misbruik worden.

Beslismodellen mogen niet getraind worden op generieke kenmerken.

Er komen regels over de kwaliteit en het type data dat gebruikt mag worden voor de training van automatisch gegenereerde beslismodellen. Om te voorkomen dat beslismodellen gebruikt worden die mensen benadelen op grond van generieke kenmerken, moet de overheid eisen dat modellen alleen getraind mogen worden op kenmerken die een causaal verband kunnen hebben met de voorspelde waarde. Ook moet inzichtelijk gemaakt worden hoe de kwaliteit van de gebruikte data is en op welke manier afwegingen zijn gemaakt om discriminatie en ongelijke behandeling te voorkomen.

Er komt een wettelijk recht op uitleg bij besluiten door de overheid.

Wanneer de overheid een (geautomatiseerd) besluit heeft genomen, dient het altijd mogelijk te zijn om een uitleg van het besluit te krijgen door een ambtenaar met inhoudelijke kennis over het besluit. Computer says no mag geen eindpunt zijn. Een praktisch aspect is dat de overheid ook bereikbaar moet zijn om uitleg te geven over keuzes. Gemeenten, provincies, de Rijksoverheid en de overheidsdiensten zullen een telefonisch of fysiek loket moeten hebben waar burgers terecht kunnen met vragen over een bepaald besluit, bijvoorbeeld het weigeren van een vergunning of de toekenning van een toelage. De uitleg kan de basis zijn voor een juridisch bezwaar volgens de gebruikelijke weg.

Geen ongebreidelde dataverzameling via digitale identiteiten.

Bij de ontwikkeling van digitale identiteit dient voorkomen te worden dat deze wordt gebruikt om data te verzamelen en te verhandelen. De overheid kiest daarom voor een gedistribueerd systeem, waarbij mensen zelf controle blijven houden over welke informatie met wie gedeeld wordt. Voorkomen moet worden dat een digitale identiteit (sluipenderwijs) gaat leiden tot uitsluiting van mensen van bepaalde diensten. De overheid zal daarom vooraf duidelijk moeten definiëren wat het doel en de functie van een digitale identiteit is, op basis van een zorgvuldige waarden- en belangenafweging. Ook moet de overheid zorgen dat er alternatieven blijven voor mensen die geen gebruik kunnen of willen maken van digitale identiteit.

Op Europees niveau moeten regels opgesteld worden over interoperabiliteit tussen digitale diensten, zodat 'opsluiting in ecosystemen' voorkomen wordt.

Techbedrijven worden verplicht om hun diensten open te stellen voor mensen die ook diensten elders afnemen, en andersom, het mogelijk te maken voor hun klanten een deel van de diensten bij andere bedrijven af te nemen. Concreet: je moet een operating system kunnen gebruiken zonder de facto

verplicht te worden de browser van dezelfde aanbieder te gebruiken; je moet een telefoon kunnen gebruiken zonder verplicht een e-mailadres bij een bedrijf af te nemen, en je moet een vrije keuze hebben welke cloudservice je telefoon gebruikt voor je foto's. Dit vereist interoperabiliteit van diensten, bijvoorbeeld door gebruik te maken van open API's (interfaces waarmee computersystemen met elkaar worden verbonden).

Datajubeljaar: het moet voor burgers makkelijk worden om vernietiging van hun gegevens af te dwingen, zodat een nieuwe start mogelijk is.

In de AVG staat dat gegevens tijdig moeten worden vernietigd en niet onnodig moeten worden bewaard. De overheid moet erop toezien dat bedrijven en organisaties dit doen. Om misbruik van digitale gegevens te voorkomen en een nieuwe start te faciliteren, moet de overheid regels ontwikkelen die burgers het recht geven hun gegevens te laten vernietigen. Dit zou bijvoorbeeld een standaardaanbod kunnen worden aan 18-jarigen, zodat zij met een schone digitale lei aan hun volwassenheid kunnen beginnen. Ook zou de overheid moeten stimuleren dat er meer technische mogelijkheden komen om digitaal gegevens te verstrekken die na verloop van een zekere tijd onleesbaar worden – zoals ook Snapchat doet met foto's.

Bijlage – Waar gaat het over?

Om richting te kunnen geven aan keuzes waarvoor politici gesteld worden, is het belangrijk om goed te weten waar we over spreken. Digitalisering is een breed begrip met allerlei toepassingen. In deze bijlage bespreken we een aantal begrippen en technische aspecten dat relevant is in de politieke dilemma's. Voor wie voldoende technische achtergrondkennis heeft, is deze bijlage niet essentieel.

Hooggespannen verwachtingen

Laten we allereerst kijken naar de manier waarop technologie haar weg vindt in de maatschappij. Vaak gaan nieuwe technologieën gepaard met hooggespannen verwachtingen, maar die komen niet altijd uit. Toen cameratoezicht en gezichtsherkenning zijn intrede deed, werd gedacht dat daarmee elke winkeldief en voetbalvandaal uit de massa gevestigd kon worden. Die praktijk bleek weerbarstig, maar inmiddels is het wél zo ver, dat met cameratoezicht en kentekenherkenning de moordenaars van Peter R. de Vries direct staande konden worden gehouden. Toen de algoritmische besluitvorming zijn intrede deed bij de overheid, was er vooral enthousiasme: 'nu kunnen we fraude opsporen!' De toeslagenaffaire heeft dat beeld doen kantelen. Er zijn rond de invoering van nieuwe technologieën vaste patronen te herkennen, die ook relevant zijn in politieke besluitvorming. Bekend is de zogeheten Hype Cycle van Gartner. Dit model tekent hoe een opkomende technologie na de eerste successen vaak gehypet wordt. Politiek en bestuur gaan daar soms in mee. De verwachtingen zijn dan (te) hoog. Alles is op te lossen! Alles wordt anders! Wat volgt is teleurstelling als de praktijk weerbarstig blijkt. Toch volgen vaak ruim na de hype-fase bruikbare toepassingen, al zijn ze niet zo alomvattend als eerder gedacht.

Nauw verwant is de zogeheten wet van Amara (Amara's law), vernoemd naar de vroegere president van het Amerikaanse Institute for the Future (ITF). Deze wet gaat over de impact van technologie en stelt dat met betrekking tot (nieuwe) technologie de effecten op korte termijn altijd worden overschat, terwijl de effecten op lange termijn altijd worden onderschat. Een derde patroon, specifiek voor ICT, is dat de invoering van technologie vaak begint met de digitalisering en automatiseren van bestaande situaties terwijl vervolgens andere werkwijzen en nieuwe opleidingsbehoeften ontstaan.

Wat is er eigenlijk nieuw?

Het opslaan en verwerken van gegevens gebeurt al millennia lang. Meestal gaat het om hetzelfde principe: het opschrijven of het maken van een inscriptie in een materiële drager: van kleitablet tot A4-papier. Door informatie in reeksen van 0 en 1 te coderen, is het mogelijk veel meer te doen met de informatie dan alleen het registreren. Er zijn verschillende technologische ontwikkelingen geweest die daaraan hebben bijgedragen. Met de doorbraak van de computer in de jaren tachtig van de vorige eeuw is het registreren en opslaan van gegevens makkelijker geworden. De komst van het internet heeft ervoor gezorgd dat uitwisseling van gegevens een stuk sneller en grootschaliger kon plaatsvinden. Het steeds bredere gebruik van digitale technologie heeft er ook toe geleid dat er steeds meer gegevens beschikbaar kwamen, bijvoorbeeld uit sensoren, camera's of door registratie van online activiteiten. Ten slotte heeft de groei van rekenkracht en opslagcapaciteit van computers ervoor gezorgd dat we steeds beter in staat zijn om digitale gegevens te interpreteren en op basis hiervan voorspellingen te doen, bijvoorbeeld met modellen die werken met kunstmatige intelligentie. Digitalisering heeft dus gezorgd voor een enorme versnelling en verbreding van het gebruik van gegevens. Dit maakt dat er op veel grotere schaal mee kan worden gewerkt. Waar dat vroeger monnikenwerk was, kunnen nu eenvoudig duizenden dossiers met elkaar worden vergeleken en onderzocht op afwijkingen.

Internet: surface, deep en dark web

Digitalisering is mogelijk omdat het internet alles aan elkaar knoopt. Met 'het internet' worden in de volksmond vaak alle websites bedoeld die je kunt vinden met een zoekmachine (het world-wide-web: www). Dit wordt ook wel het 'surface web' genoemd omdat dit maar een fractie is van wat er allemaal 'online' staat. Er zijn nog veel meer computergegevens via internet bereikbaar, die niet voor direct men-

selijk gebruik zijn bedoeld, maar gericht zijn op computers. Je komt daar alleen bij als je het goede adres weet, de juiste computertaal hanteert en (soms) inloggegevens gebruikt. Steeds meer overheidsorganisaties delen hun gegevens; dit wordt 'open data' genoemd. Hierdoor wordt het mogelijk voor computers om gegevens van andere organisaties te gebruiken. Een bekend voorbeeld is de ov-informatie: iedere vervoersmaatschappij stelt actuele informatie beschikbaar over de aankomsttijden en vertragingen van de bussen. Websites als 9292.nl kunnen daarvan gebruik maken om een reis te plannen. Deze gegevens die voor computers toegankelijk zijn, worden samen ook wel het 'deep web' genoemd. Er is een nog dieper gelegen deel van het internet, het 'dark web', waar zelfs het kennen van het adres niet voldoende is. Je hebt dan speciale software (zoals een speciale browser met versleuteling) nodig om er te komen. Dit 'dark web' wordt gebruikt voor illegaal vraag en aanbod maar ook door bijvoorbeeld klokkenluiders.

Algoritme

Een algoritme is een reeks instructies die gebruikt wordt om data te interpreteren. Een algoritme is niet speciaal intelligent: het is een instructie waar je iets in stopt en waar iets uitkomt, te vergelijken met een recept. Met algoritmes kunnen processen geautomatiseerd worden. Wanneer het in de media tegenwoordig gaat over algoritmes, wordt vaak bedoeld op algoritmes die door een computer zelf zijn ontwikkeld, via zogeheten machine learning, een techniek die valt onder kunstmatige intelligentie.

Kunstmatige Intelligentie en machine learning

Kunstmatige intelligentie (in het Engels AI) is een begrip dat niet zo heel eenvoudig te definiëren valt. We volgen de definitie van de Wetenschappelijke Raad voor het Regeringsbeleid, die AI definieert als 'systemen die intelligent gedrag vertonen door hun omgeving te analyseren en – met enige graad van autonomie – actie te ondernemen om specifieke doelen te bereiken. Deze acties zijn dan vaak beslissingen van een computer, maar het kunnen ook daadwerkelijke acties zijn wanneer AI onderdeel is van een systeem zoals een robot of auto. De output van AI kan lijken op menselijke intelligentie; de manier waarop AI tot die output komt, is echter anders dan bij mensen. Op dit moment geldt dat AI in afgebakende taken veel meer kan dan een mens (narrow AI) maar dat mensen meer vaardigheden combineren.¹⁵

Een veelgebruikte vorm van AI is machine learning. Bij machine learning worden complexe algoritmes gebouwd door de computer te laten leren van voorbeelden. Een systeem gebruikt dan bijvoorbeeld data (plaatjes van katten) om die te leren herkennen en te onderscheiden van andere data (plaatjes van honden). Hoe meer kattenplaatjes zo'n systeem ziet, hoe meer typische 'kattenkenmerken' het kan leren, en hoe beter het katten van honden kan onderscheiden.

Dit soort systemen zijn doorgaans een 'neuraal netwerk'; een programma dat de werking van hersencellen nabootst: de output van een cel beïnvloedt hoe verbonden cellen reageren, en door terugkoppeling te geven of een antwoord goed of fout is, wordt de sterkte van de verbinding tussen de verschillende cellen aangepast. In de standaardvorm bestaat het neurale netwerk waarin de analyse plaatsvindt uit een paar lagen.

Deep learning is een bijzondere vorm van machine learning die bestaat uit veel meer lagen en daarom complexere informatie kan verwerken, eventueel in verschillende detailniveaus. In feite detecteren alle machinelearningalgoritmes complexe statistische verbanden tussen de invoer (geobserveerde kenmerken) en de uitvoer (conclusie of voorspelling). Vaak is het daarbij voor mensen niet meer duidelijk waarom een combinatie van kenmerken leidt tot bepaalde conclusies (zgn. blackboxmodellen). Er wordt momenteel veel onderzoek gedaan naar manieren om deze modellen inzichtelijker te maken (explainable AI), maar dit staat nog in de kinderschoenen.¹⁶

¹⁵ Wetenschappelijke Raad voor Regeringsbeleid, Opgave AI. De nieuwe systeemtechnologie (Den Haag: WRR, 2021) 48-49.

¹⁶ René Fransen, "Kunstmatige intelligentie voor beginners", in: Groen 2021(2).

Algoritmische besluitvorming

Bedrijven en overheden maken steeds meer gebruik van digitale mogelijkheden om gegevens te verzamelen, te ordenen en te selecteren. Door de toepassing van algoritmes, zoals hierboven beschreven, wordt het steeds makkelijker om automatisch selecties te maken en voorspellingen te doen. Wanneer deze voorspellingen de basis vormen voor een besluit spreken we van algoritmische besluitvorming. Dit kan bijvoorbeeld gaan om de acceptatie van een lening, de honorering van een verzekeringsclaim of het voorspellen van criminaliteit of fraude. Vaak zie je dat een deel van de besluiten automatisch wordt genomen en de ingewikkeldere gevallen voor handmatige beoordeling worden voorgedragen. Soms worden algoritmes ingezet om te besluiten welke situaties extra controle verdienen. Automatische besluitvorming kan bijdragen aan de effectiviteit, consistentie en efficiency van besluiten. Tegelijk brengt deze vorm het risico met zich mee dat het onduidelijk is op welke grond bepaalde keuzes zijn gemaakt. Bovendien bestaat het risico dat keuzes worden gemaakt op basis van vooroordelen. Wat zelflerende systemen niet kunnen, is het verschil maken tussen correlatie (samen optreden van variabelen) en causaliteit (een oorzaak-gevolgverband). Door dit gebrek is het voorgekomen dat mensen niet op grond van hun handelen maar op basis van overeenkomsten met anderen benaderd werden, ook door overheden.

Vooroordelen en discriminatie door algoritmen

Algoritmes die door een computer worden gebruikt om voorspellingen te doen, worden ook wel (computer)modellen genoemd. Een model of algoritme kan op basis van expertkennis zijn gemaakt of op basis van machine learning. In alle gevallen geldt dat een model altijd een vereenvoudiging (abstractie) van de werkelijkheid is. Dat betekent dat bepaalde zaken zijn weggelaten. Onbewust kunnen dat ook essentiële zaken zijn, waardoor het model onbetrouwbaar wordt. Machinelearningmodellen zijn nooit beter dan de data die gebruikt zijn om hen te trainen. Garbage in is garbage out, luidt een bekend gezegde in de datawetenschap. Als de gebruikte data bijvoorbeeld gebaseerd zijn op een niet-neutrale selectie (denk aan een dataset met een overrepresentatie van inwoners uit een bevolkingsgroep), zullen de modellen de afwijkingen in de data overnemen. Als we een op basis van data / machine learning gemaakt model vragen, te voorspellen wie de volgende minister-president van Nederland is, zal het antwoord altijd bij een man uitkomen. Tot nu toe waren alle minister-presidenten (de voorbeelden waarvan is geleerd) immers man. Dit fenomeen wordt beschreven met de Engelse term bias. Het lijkt vooralsnog een illusie dat we lerende systemen kunnen maken zonder bias. Het is zelfs heel ingewikkeld om te bepalen of een systeem een bias heeft. We weten immers niet of we iets missen en zullen er dus altijd op bedacht moeten zijn.

Generatieve AI: perfecte namaak

Naast voorspellingen doen over data, zien we ook steeds meer toepassingen op het gebied van generatieve AI: toepassingen waarbij de algoritmen worden gebruikt om nieuwe informatie samen te stellen. Dat kan bijvoorbeeld gaan om het maken van realistische portretfoto's van mensen die niet bestaan (<https://this-person-does-not-exist.com/en>), of het maken van kunstwerken in een bepaalde stijl (<https://openai.com/dall-e-2/>) tot aan het voorspellen van eiwitstructuren.

Generatieve AI wordt ook gebruikt om filmpjes te maken: deepfakes. Een deepfake is een afbeelding of film waarin mensen voorkomen in een niet-bestaande situatie. Politici kunnen erin figureren en teksten uitspreken die met hun eigen stem gemanipuleerd zijn. Het overgrote deel van deepfakes bestaat uit filmpjes van mensen, vooral vrouwen, van wie het gezicht ongewild in een pornofilm gemonteerd is.

Het is ook mogelijk om coherente teksten te genereren die op het eerste gezicht overtuigend zijn. Op 20 november 2022 werd ChatGPT van het bedrijf OpenAI publiek toegankelijk. Het programma kan in code schrijven, maar ook gedichten genereren, recepten verzinnen en grapjes produceren.

In bovenstaande gevallen genereert het algoritme een uitvoer die gebaseerd is op een grote hoeveel-

heid statistische informatie over kenmerken die vaak bij elkaar voorkomen. Het gaat dus eerder om het berekenen van output dan om het bedenken ervan.

Autonome systemen

Als een computer zelfstandig keuzes maakt of een actie uitvoert, spreken we van een autonoom systeem. Zo hebben automodellen vanaf mei 2018 in de EU verplicht het e-callysteem, dat zelf 112 belt en locatiegegevens deelt met hulpdiensten wanneer de auto een harde botsing maakt. Een heel andere toepassing is een autonoom wapensysteem dat op basis van geprogrammeerde regels en methodes zelfstandig zoekt naar doelen en die kan aanvallen, in de volksmond 'killer robots' genoemd. Dit roept de vragen op wat autonomie precies is en wie verantwoordelijk is wanneer een autonoom systeem verkeerde keuzes maakt.

Sociale media

Sociale media zijn online platformen waarop de gebruikers, zonder of met minimale tussenkomst van een professionele redactie, informatie met elkaar delen. Vaak is de manier waarop informatie verspreid wordt deels afhankelijk van de verbindingen die gebruikers met elkaar zijn aangegaan, bijvoorbeeld door iemand als 'vriend' aan te merken, of door iemand te 'volgen'. Het kan bijvoorbeeld gaan om het uitwisselen van foto's (Instagram, Snapchat), filmpjes (TikTok, YouTube) of korte tekstberichten (Twitter). De sociale media kopiëren functionaliteit van elkaar en veel platformen bieden een combinatie van dit soort mogelijkheden.

Vrijwel alle grote socialemediaplatformen maken gebruik van kunstmatige intelligentie om de voorkeuren van gebruikers te kennen, en op die manier informatie te tonen die aansluit bij de interesses van de gebruikers. Vaak is het doel daarvan om de tijd te verlengen die gebruikers op het platform besteden. Immers, hoe langer gebruikers tijd spenderen op het platform, hoe meer mogelijkheden er zijn om advertenties te tonen en daarmee geld aan de gebruiker te verdienen. Socialemediaplatformen gebruiken allerlei data voor het leren van voorkeuren, bijvoorbeeld hoe lang gebruikers kijken naar bepaalde informatie, wat ze zoeken, hoe snel ze klikken, maar vaak ook informatie over de websites die ze bezoeken, naar welke onderwerpen ze zoeken op internet, wat hun vrienden bekijken en welke andere apps ze gebruiken.

De personalisatie op basis van kunstmatige intelligentie kan er ook toe leiden dat gebruikers eenzijdige informatie getoond krijgen. Experimenten hebben laten zien dat na relatief korte tijd de getoonde informatie zeer specifiek is (soms wel een rabbit hole of fabeltjesfuik genoemd). De vergaande personalisatie van de getoonde informatie, gecombineerd met functies zoals het automatisch tonen van volgende filmpjes of het oneindig door kunnen scrollen, kan bijdragen aan verslaving aan het gebruik van sociale media.

Blockchain en cryptocurrency

Blockchain is een techniek waarmee door een wereldwijd netwerk van computers gezamenlijk een lijst van acties wordt bijgehouden (een ketting van blokjes informatie). Het systeem is te zien als een soort logboek waarmee niet geknoeid kan worden, omdat honderden mensen een kopie hebben en deze mensen iedere keer als er iets bijgeschreven wordt, eerst met elkaar afstemmen of ze er allemaal nog dezelfde informatie in hebben staan. De informatie zelf kan wel versleuteld zijn. Omdat het logboek op veel plekken tegelijk wordt bewaard, kan informatie niet veranderd, verduisterd of afgeschermd worden. Er is namelijk niet één persoon of organisatie die de eigenaar is. De technologie is daarmee uitermate geschikt om gezamenlijk afspraken vast te leggen zonder dat er een centrale autoriteit nodig is om de afspraken te controleren.

Deze technologie maakt allerlei toepassingen mogelijk. De bekendste daarvan is de Bitcoin, een digitaal

muntsysteem waarbij de blockchaintechnologie wordt gebruikt om bij te houden wie hoeveel Bitcoins aan wie betaalt. Een centrale bank is dan niet meer nodig, want iedereen kan zien welke transacties zijn uitgevoerd. Naast de Bitcoin zijn er allerlei andere cryptocurrencies, die gebaseerd zijn op de blockchaintechnologie. Omdat cryptocurrencies niet afhankelijk van een centrale bank zijn, kan een parallel geldsysteem ontstaan. Het feit dat informatie versleuteld is, zorgt er bovendien voor dat digitaal geld volledig anoniem kan worden uitgewisseld. Deze anonimiteit maakt cryptocurrencies ook voor criminele activiteiten aantrekkelijk.

Andere mogelijke toepassingen van blockchain zijn het foutloos registreren en uitwisselen van medische data, of het bijhouden van auteursrechten van digitale informatie. Hoewel er veel mogelijke toepassingen genoemd worden, wordt ook steeds duidelijker dat blockchain niet voor alle problemen de meest geschikte techniek is.

Om de gegevens in een blockchain aan te vullen en te controleren, is veel rekenkracht van veel computers nodig en dat kost veel elektriciteit. Geschat wordt dat het totale energieverbruik van alleen de blockchain die Bitcoin gebruikt, gelijk is aan het totale stroomverbruik van een land als Zwitserland.

Digitale identiteit

Een digitale identiteit (of digitaal paspoort) is een term voor een app of toepassing waarmee je kunt aantonen wie je bent. Een bekende toepassing is de DigiD, waarmee je kunt inloggen op websites van de overheid. Andere voorbeelden zijn functies die bedrijven zoals Facebook of Google bieden om in te loggen bij websites van derden, of de eHerkenningdienst waarmee bedrijven zich online identificeren. Digitale identiteiten bestaan dus al en worden veel gebruikt.

De discussie over digitale identiteit gaat daarom vaak niet over de identificatiefunctie op zichzelf, maar over wie de toepassing beheert, welke informatie wordt opgeslagen en gedeeld, en in welke situaties identificatie gevraagd mag worden. Het maakt immers verschil of de landelijke overheid de identiteit beheert, de Europese Unie, of een commercieel bedrijf dat door haar vestiging al dan niet binnen onze rechtsstaat valt. Bovendien kunnen verschillende keuzes worden gemaakt over de informatie die in het digitale paspoort wordt opgeslagen. Bij een toepassing als DigiD wordt zeer beperkt informatie opgeslagen (de meeste informatie zit niet in e-identity, maar in de afzonderlijke systemen van de overheid), maar bedrijven zoals Google houden veel informatie bij in hun digitale paspoort, en delen die ook met websites waarop je inlogt. Zelfs als een digitaal paspoort nauwelijks informatie bevat, kunnen de meta-data (wanneer gebruikt iemand zijn e-identity? voor welke toepassing?) worden verzameld.

Er zijn technische oplossingen voor e-identity waarbij er geen informatie in een centraal systeem wordt opgeslagen.¹⁷ In plaats daarvan blijft die informatie bij de gebruiker zelf en kan de gebruiker voor iedere specifieke situatie aangeven welke informatie gedeeld mag worden. Bijvoorbeeld, als je alcoholische drank wilt kopen, geef je de app alleen toestemming om te vertellen dat je ouder dan achttien bent, zonder je geboortedatum te onthullen of je adres. Een digitale identiteit staat dus niet per definitie op gespannen voet met privacy.

Een e-identity staat wel op gespannen voet met anonimiteit. Hoe meer toepassingen identificatie vereisen, hoe minder je anoniem gebruik kunt maken van diensten. Bovendien maakt een digitale identiteit het een stuk makkelijker om digitale gegevens die over een persoon beschikbaar zijn met elkaar te verbinden.

¹⁷ Zie bijvoorbeeld <https://privacybydesign.foundation/irma-uitleg/>.

Cybersecurity

Cybersecurity gaat over de beveiliging van digitale systemen tegen aanvallen door kwaadwillenden. Vanwege de essentiële functie van digitale technologie voor het functioneren van de samenleving zijn er grote consequenties wanneer een systeem, een website of zelfs het hele internet in een gebied aangevallen wordt. Waterveiligheid, de energievoorziening, het gebruik van ov en snelwegen, en het financiële verkeer zijn vrijwel uitsluitend digitaal vormgegeven. Ook bedrijfslogistieke processen zijn veelal digitaal. Terwijl traditionele criminaliteit afneemt, neemt cybercrime sterk toe en vinden er steeds meer aanvallen plaats op digitale systemen van overheden, bedrijven en instellingen als universiteiten en ziekenhuizen. Door in te breken op systemen kunnen systemen worden platgelegd, kan informatie worden gestolen of veranderd, of kunnen gegevens worden gegijzeld in ruil voor geld. In 2020 werd bijvoorbeeld de gemeente Hof van Twente gehackt met gijzelsoftware waardoor de gemeente ruim vier miljoen euro schade leed. Aanvallen kunnen gebeuren uit persoonlijke belang (bijvoorbeeld op een illegale manier geld te verkrijgen) of uit (geo)politiek belang.

Privacy

Privacy gaat over het recht op een persoonlijke levenssfeer: het recht om te leven zonder onnodige inmenging in die sfeer door anderen: van overheden en bedrijven tot de overbuurvrouw. Onderdeel ervan is het recht op bescherming van persoonsgegevens. Het recht op privacy is niet absoluut en er zijn veel redenen die rechtvaardigen dat inbreuk wordt gemaakt op de persoonlijke levenssfeer. De inbreuk mag niet groter zijn dan noodzakelijk. Eén van de meest bekende risico's van digitalisering is dat de persoonlijke levenssfeer meer dan nodig wordt aangetast. Want doordat we steeds meer activiteiten uitvoeren via computers en telefoons, wordt er steeds meer informatie geregistreerd en opgeslagen over wat wij doen, en wordt de ruimte waarin wij ons ongezien weten, steeds kleiner. Het is daarom belangrijk om zorgvuldig met de verzameling en het beheer van persoonlijke (digitale) gegevens om te gaan.

Algemene verordening gegevensbescherming (AVG)

De Europese Unie ziet het belang van gegevensbescherming en heeft daarom regels opgesteld over de omgang met persoonlijke gegevens. Sinds 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat in de hele Europese Unie (EU) dezelfde privacywetgeving geldt. Hoewel de uitgangspunten van de AVG veelbelovend zijn, schiet de handhaving vooralsnog tekort. De belangrijkste beginselen uit de AVG zijn als volgt samen te vatten.

- De verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn;
- de persoonsgegevens mogen alleen worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden;
- er mogen niet meer persoonsgegevens worden verwerkt dan noodzakelijk zijn voor deze doelen;
- de persoonsgegevens moeten juist zijn;
- de persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk;
- en de integriteit en vertrouwelijkheid van de persoonsgegevens moet voldoende worden beschermd.

Leestips

Wetenschappelijke Raad voor het Regeringsbeleid, *Opgave AI. De nieuwe systeemtechnologie*, Rapport nr. 105 (Den Haag, 2021)

<https://www.wrr.nl/publicaties/rapporten/2021/11/11/opgave-ai-de-nieuwe-systeemtechnologie>

Raad van State, *Ongevraagd advies over de effecten van de digitalisering voor de rechts-statelijke verhoudingen* (Den Haag, 2018)

<https://www.raadvanstate.nl/@112661/w04-18-0230/>

Rathenau Instituut, *Algoritmes afwegen. Verkenning naar maatregelen ter bescherming van mensenrechten bij profilering in de uitvoering* (Den Haag, 2022)

<https://www.rathenau.nl/nl/digitalisering/algoritmes-afwegen>

Maxim Februari, *Doe zelf normaal. Menselijk recht in tijden van datasturing en natuurgeweld*. Amsterdam: Prometheus 2023

Bibliografie

J. Boersma (2022). "Je identiteit is geen paspoort" (blog). Website: <https://edi.pleio.nl/groups/view/b3d6dbc0-959c-4c07-9048-14fb9f736bcd/edi-algemeen/blog/view/92e5bf83-3909-4387-b2b7-8d3ad-df0fc28/opinie-je-identiteit-is-geen-paspoort>.

ChristenUnie (2018). *Vrede zoeken, recht doen. Beginselverklaring van de ChristenUnie*. Website: <https://www.christenunie.nl/beginselverklaring>.

Fransen, R. (2021). "Kunstmatige intelligentie voor beginners". Groen 2021(2).

Keles, B, N. McCrae & A. Grealish. 'A systematic review: the influence of social media on depression, anxiety and psychological distress in adolescents', *International Journal of Adolescence and Youth* 2020, 25(1).

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

Raad voor de Leefomgeving (2021). *Digitaal duurzaam*. Website: <https://www.rli.nl/publicaties/2021/advies/digitaal-duurzaam>.

Raad van State (2018). *Ongevraagd advies over de effecten van de digitalisering voor de rechtsstatelijke verhoudingen*. Kamerstukken II 2017/18, 26643, nr. 557. Website: <https://www.raadvanstate.nl/@112661/w04-18-0230/>

Rijksoverheid (2021). "Hack bij Waterschap kan voor serieuze dreiging zorgen". Website: <https://www.digitaleoverheid.nl/achtergrondartikelen/hack-bij-waterschap-kan-voor-serieuze-dreiging-zorgen/>.

Schuurman, D. *Shaping a Digital World. Faith, Culture and Computer technology*. Westmont: IVP Academic Publishing 2013.

Schuurman, E. *Transformation Of the Technological Society*. Sioux Center: Dordt Press 2022.

Wetenschappelijke Raad voor Regeringsbeleid (2021). *Opgave AI. De nieuwe systeemtechnologie*. Rapport 105. Den Haag: WRR. Website: <https://www.wrr.nl/adviesprojecten/artificiele-intelligentie/documenten/rapporten/2021/11/11/opgave-ai-de-nieuwe-systeemtechnologie>

CONTACTGEGEVENS

Partijbureau ChristenUnie
Postbus 439
3800 AK AMERSFOORT
Telefoon: 033-4226969
E-mail: info@christenunie.nl

Wetenschappelijk Instituut
Postbus 439
3800 AK AMERSFOORT
E-mail: wi@christenunie.nl

MEER DAN ENEN EN NULLEN

Digitaliseringsvisie
April 2023

Christen
Unie

wi Wetenschappelijk
Instituut
ChristenUnie