

# De tien pijlers van het Nederlandse techniekbeleid

Bart van der Sloot<sup>1</sup>

Algoritmen, *big data*, *deepfakes*, kunstmatige intelligentie, *personalised medicine* en *smart cities*. Het is slechts een kleine greep uit de vele digitale technieken en toepassingen die de Nederlandse samenleving het laatste decennium mede hebben vormgegeven. Naar aanleiding van onder meer de invloed van fake news op de Amerikaanse verkiezingen, de datamacht van een klein aantal internetondernemingen en de toeslagenaffaire is er steeds meer oog voor de noodzaak om data-gedreven innovatie in te kaderen. Dit artikel analyseert op welke fundamenten het Nederlandse beleid is gestoeld en welke visie op technologie, de digitale samenleving en de rol van het recht daaraan ten grondslag ligt.

## Inleiding

Nederland behoort tot de meest gedigitaliseerde samenlevingen ter wereld, waarin steeds meer interactie met en processen binnen de publieke en de private sector worden bepaald of gemedieerd door techniek. De overheid heeft deze ontwikkeling met het oog op innovatie, vooruitgang en werkgelegenheid lange tijd eerder aangemoedigd dan afgeremd. Door de maatschappelijke onrust rondom de toeslagenaffaire en de zorgen omtrent onder meer privacy, vrijheid van meningsuiting en discriminatie op sociale media neemt de overheid een steeds actievare rol in het begeleiden van digitalisering en het inkaderen van techniek in. Onlangs culmineerde dat in de meer dan 50 pagina's tellende Werkagenda Waardengedreven Digitaliseren.<sup>2</sup>

Een goed moment dus om de balans op te maken. Wat zijn eigenlijk de uitgangspunten van de Nederlandse benadering van digitale technologie, wie zijn daarin de primaire normadressaten en welk type regels wordt doorgaans opgelegd? Vaak is er aandacht voor een specifieke technologie, de gevolgen daarvan en de eventuele noodzaak tot wetgeving, maar blijven de algemene uitgangspunten van het Nederlandse techniekbeleid buiten beschouwing, terwijl juist die bepalend zijn voor de uiteindelijke reguleringskeuze. Uit een analyse van wetgevingstrajecten, Kamerbrieven en kabinetsreacties uit het afgelopen decennium zijn tien fundamenten van het Nederlandse techniekbeleid te destilleren: (1) terughoudendheid bij eventuele wetswijzigingen, (2) het geloof dat techniek als zodanig neutraal is en (3) dat digitalisering en technologisering de samenleving ten goede komen, (4) de wens om zowel de kool (het recht) als de geit (de technologie) te sparen, (5) een voorkeur voor expost regulering, (6) een nadruk op de bescherming van individuele in plaats van algemene belangen, (7) het

geloof in de regierol van de burger, (8) de keuze om het reguleringsinitiatief bij 'Europa' te laten, (9) regelgeving vervolgens zo open mogelijk te houden en (10) de wens te komen tot een kleine publieke sector.

Naast een beschrijving van de dominante beleidslijn en de ideologie die daaraan ten grondslag ligt zal worden gekeken naar eventuele alternatieve reguleringsstrategieën. Welke lessen kan de wetgevende macht trekken uit de analyse van de reguleringskeuzes van het afgelopen decennium bij het ontwikkelen van toekomstig digitaliseringsbeleid?

## 1. Behoedzaamheid

Een belangrijk kenmerk van techniekregulering in Nederland is het grote aantal adviezen die soms ongevraagd maar meestal gevraagd aan de regering worden gegeven door de diverse adviesraden en kennisinstututen en het minstens even grote aantal wetenschappelijke onderzoeken dat wordt uitgezet via het Ministerie van Binnenlandse Zaken en het Wetenschappelijk Onderzoeks- en Documentatiecentrum (WODC). Zo verschenen er alleen al bij het WODC in het tijdsbestek van een jaar onderzoeken naar virtuele valuta,<sup>3</sup> strafvorderlijke gegevensverwer-

### Auteur

1. Dr. B. van der Sloot is Universitair hoofddocent aan het Tilburg Institute for Law, Technology and Society (TILT) van Tilburg University.

### Noten

2. *Werkagenda Waardengedreven Digitaliseren*, bijlage bij *Kamerstukken II 2022/23*,

26643, nr. 940, open.overheid.nl/repository/ronl-0de79e5c4c0c9b203c0a1c263ef-ca7eca410958b/1/pdf/bijlage-1-werkagenda-waardengedreven-digitaliseren.pdf.

3. V. Schrama et al. (2022), *Virtuele valuta*, WODC-rapport 3184, repository.wodc.nl/handle/20.500.12832/3215.



© Shutterstock

king,<sup>4</sup> ransomware-aanvallen,<sup>5</sup> hackbevoegdheden,<sup>6</sup> persoonsgegevens,<sup>7</sup> veilig wachtwoordgedrag,<sup>8</sup> kinderseksrobots,<sup>9</sup> neurotechnologie,<sup>10</sup> cameratoezicht,<sup>11</sup> deepfakes,<sup>12</sup> games,<sup>13</sup> webharvesting,<sup>14</sup> passagiersgegevens,<sup>15</sup> cybercriminaliteit<sup>16</sup> en kentekenregistratie.<sup>17</sup>

Op geen ander beleidsterrein verschijnen zoveel rapporten, adviezen en handreikingen. Daar valt wat voor te

zeggen. Technologie is complex en hoe het staande juridische kader ingrijpt op nieuwe technologieën is niet altijd eenduidig vast te stellen; alternatieven voor of aanvullingen op bestaande wetgeving hebben vrijwel altijd voor- en nadelen en vragen soms een brede heroriëntatie op juridische doctrines. Het kan daarom raadzaam zijn om alvorens wetswijzingen voor te stellen een onafhankelijk

# De Nederlandse regering zet de onderzoeken zelden proactief uit, maar vaak pas jaren nadat een techniek in gebruik is genomen

oordeel te vragen van experts met een technische of juridische achtergrond. Deze benadering heeft desalniettemin een nadeel, dat juist bij techniekregulering van groot belang is, namelijk vertraging. Des te langer een techniek zich ongebreideld kan ontwikkelen, des te moeilijker het wordt deze nog bij te sturen; ook betekent het dat de eventuele negatieve consequenties van een technologie zich lopende het onderzoek blijven manifesteren. Daarbij valt op dat de Nederlandse regering de onderzoeken zelden proactief uitzet, maar vaak pas jaren nadat een techniek in gebruik is genomen.

Een voorbeeld is de regulering van *deepfake*-technologie. De term *deepfake* is zo rond 2017 gemunt en de techniek heeft in een klein aantal jaren een sterke ontwikkeling doorgemaakt, waardoor professionele *deepfakes* niet meer van echt te onderscheiden zijn. De techniek wordt voor het eerst in 2019 in de Kamer besproken door de voorzitter van de Autoriteit Persoonsgegevens<sup>48</sup> en het kabinet gebruikt de term vervolgens zelf in reactie<sup>49</sup> op het rapport *Zoeken naar waarheid* van de Raad voor Openbaar Bestuur.<sup>20</sup> Uit-

eindelijk wordt eind 2020 via het WODC een wetenschappelijk onderzoek naar dit fenomeen uitgezet, dat eind 2021 is opgeleverd en waar het kabinet naar verluidt eind 2022 op zal reageren. Zelfs als het kabinet voornemens zou zijn wetgeving te introduceren, dan zal die pas in 2023 in stemming worden gebracht en op zijn vroegst in 2024 in werking treden. Dat is anders dan in andere landen, zoals de Verenigde Staten en China, waar al jaren geleden wetgeving op dit punt is aangenomen.

Behoedzaamheid als het gaat om wetswijzingen valt ook te zien in het fenomeen dat de regering de suggesties uit de aangevraagde adviezen om tot wetswijzingen over te gaan zelden overneemt, vaak met de opmerking dat het bestaande juridische kader haars inziens voldoende geëquipeerd is om de kwalijke gevolgen van technologie te adresseren, en dat als er bij de Kamer toch animo lijkt te bestaan voor een van de in de rapporten geopperde reguleringsopties, het kabinet bij voorkeur eerst nog een onderzoek laat verrichten.<sup>21</sup> Zo besprak de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) in een rapport over *big data* uit 2016 de mogelijkheid om ook de verwerking van gegevens niet zijnde persoonsgegevens in te kaderen (die nu vrijwel ongereguleerd zijn).<sup>22</sup> Het kabinet zegde daarop toe deze optie verder uit te laten werken, wat resulteerde in een WODC-rapport dat eind 2019 verscheen.<sup>23</sup> In reactie daarop werd vervolgens nog een onderzoek uitgezet op datzelfde thema, dat eind 2022 verscheen.<sup>24</sup> De WRR stelde ook voor het kader voor collectieve en algemeen belangacties uit te breiden, een optie die verder is uitgewerkt in hetzelfde WODC-rapport uit 2019, wat de regering ertoe bracht om ook op dit punt nog een additioneel WODC-onderzoek aan te vragen, dat nog loopt.<sup>25</sup>

4. M.I. Fedorova et al. (2022), *Strafvorderlijke gegevensverwerking: Een verkennende studie naar de relevante gezichtspunten bij de normering van het verwerken van persoonsgegevens voor strafvorderlijke doeleinden*, WODC-rapport 3231, repository.wodc.nl/handle/20.500.12832/3214.

5. R. Brennenraedts et al. (2022), *Verkenning risicofactoren ransomware-aanvallen*, WODC-rapport 3275, repository.wodc.nl/handle/20.500.12832/3203.

6. A.V. Uden et al. (2022), *De hackbevoegdheid in de praktijk*, Cahiers 2022-08, WODC 3106B, repository.wodc.nl/handle/20.500.12832/3202.

7. H. Winter et al. (2022), *Bescherming gegeven?*, WODC-rapport 3249, repository.wodc.nl/handle/20.500.12832/3193.

8. E.T. Mors et al. (2022), *Veilige toegang en verantwoord delen: Psychologische determinanten van veilig wachtwoordgedrag en het veilig online delen van persoonsgegevens*, WODC-rapport 3215, <https://repository.wodc.nl/handle/20.500.12832/3192>.

9. E. Loibl et al. (2022), *Quickscan wetgeving kindersekspoppen en kinderseksrobots*, WODC-rapport 3293, repository.wodc.nl/handle/20.500.12832/3189.

10. J. Bijlsma et al. (2022), *Kansen en risico's van de toepassing van neurotechnologie in het strafrecht*, WODC-rapport 3144, repository.wodc.nl/handle/20.500.12832/3174.

11. S. Flight et al. (2022), *Cameratoezicht door gemeenten*, WODC-rapport 3226, repository.wodc.nl/handle/20.500.12832/3169.

12. B. van der Sloot, Y. Wagenveld & B.J. Koops (2021), *Deepfakes*, WODC-rapport 3137, repository.wodc.nl/handle/20.500.12832/3134.

13. A. Tuijnman, R. Andree & A. J. van Rooij (2021), *Risico's, voordelen en regulering van games*, WODC-rapport 3120, repository.wodc.nl/handle/20.500.12832/3127.

14. M. R. F. Senfleben et al. (2021), *Webharvesting*, WODC-rapport 3142, repository.wodc.nl/handle/20.500.12832/3119.

15. K. Irion et al. (2021), *Evaluatie PNR-Wet*, WODC-rapport 3181, repository.wodc.nl/handle/20.500.12832/3118.

16. C. A. J. van den Eeden et al, *Opsporen, vervolgen en tegenhouden van cybercriminaliteit*, WODC Cahiers 2021-23, repository.wodc.nl/handle/20.500.12832/3114.

17. J. J. van Berkel, *Evaluatie ANPR-wetgeving 126ij Wetboek van Strafvordering*, WODC Cahiers 2021-19, repository.wodc.nl/handle/20.500.12832/3102.

J.J. Van Berkel, A. van Uden & C. J. De Poot (2021), *Tweede monitorronde evaluatie ANPR-wetgeving 126ij Wetboek van Strafvordering: De wet 'vastleggen en bewaren van kentekengegevens door de politie twee jaar in werking*, WODC Cahiers 2021-20, repository.wodc.nl/handle/20.500.12832/3103.

18. *Kamerstukken II* 2019/20, 35229, nr. 3.

19. *Kamerstukken II* 2019/20, 35300 VII, nr. 88.

20. Raad voor het Openbaar Bestuur, *Zoeken naar waarheid*, 2019.

21. Mogelijk speelt hier ook een gebrekkige kennis op het gebied van digitalisering (pijler 10) en voorkeur om digitale techniek zoveel mogelijk vrij te laten (pijlers 3 en 4).

22. WRR, *Big Data in een vrije en veilige samenleving*, rapport nr. 95, 2016, [wrr.nl/adviesprojecten/big-data-privacy-en-veiligheid/documenten/rapporten/2016/04/28/big-data-in-een-vrije-en-veilige-samenleving](http://wrr.nl/adviesprojecten/big-data-privacy-en-veiligheid/documenten/rapporten/2016/04/28/big-data-in-een-vrije-en-veilige-samenleving).

23. B. van der Sloot & S. van Schendel (2019), *De Modernisering van het Nederlands Procesrecht in het licht van Big Data. Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving*, TILT/WODC, Tilburg, WODC-rapport 2900, repository.wodc.nl/handle/20.500.12832/2390.

24. B. van der Sloot, S. Van Schendel & C.A.F. López (2022), *The influence of (technical) developments on the concept of personal data in relation to the GDPR*, WODC-rapport 3224, repository.wodc.nl/bitstream/handle/20.500.12832/3229/3224-influence-of-technical-developments-on-concept-personal-data-full-text.pdf?sequence=1&isAllowed=y.

25. *Nut en noodzaak om te komen tot een processenfonds*, WODC, projectnummer 3279, [wodc.nl/onderzoek-in-uitvoering/welk-onderzoek-doen-we/3279---nut-en-noodzaak-om-te-komen-tot-eeen-processenfonds](http://wodc.nl/onderzoek-in-uitvoering/welk-onderzoek-doen-we/3279---nut-en-noodzaak-om-te-komen-tot-eeen-processenfonds).

## 2. Techniekneutraliteit

Uit de diverse Kamerbrieven, beleidsnota's en discussies met de Tweede Kamer blijkt dat de regering digitale technologie als een intrinsiek neutraal instrument beschouwt. Ze spreekt uitsluitend in termen van kansen en risico's, voor- en nadelen of mogelijkheden en uitdagingen. Een digitale techniek is niet goed of fout, zo lijkt de gedachte, maar kent bonafide en malafide toepassingen. Uit een analyse van de voor- en nadelen van een digitale techniek volgt automatisch de vervolgvraag: hoe kan het recht zo worden ingezet dat de kansen worden benut en de risico's worden gemitigeerd?

Alhoewel het voordeel van deze benadering is dat er met een open blik naar technologie wordt gekeken, is het nadeel dat het lastig is om grotere maatschappelijke verschuivingen in kaart te brengen. Sommige experts voorspellen bijvoorbeeld een wereld van Singularity, waarin mens en machine een worden, en anderen een wereld waarin de mens in zijn geheel wordt vervangen door de machine. De vraag lijkt niet zozeer wat daarvan de kansen en risico's zijn, maar: willen we dat? Zo'n ontwikkeling ontstijgt een utilitaire belangenafweging waarin voor- en nadelen tegen elkaar worden afgewogen. Daarnaast is de vraag of techniek ook echt neutraal is. Techniek is doorgaans ontworpen met het oog op bepaalde toepassingen en dus uitermate geschikt voor die toepassingsdoeleinden. Vuurwapens zijn bijvoorbeeld ontworpen en uitermate geschikt om schade aan te richten; dat is ook de reden dat het bezit daarvan sterk aan banden is gelegd.

Ook sommige digitale technologieën zijn primair ontwikkeld met het oog op kwalijke toepassingen en worden voornamelijk daarvoor ingezet, zo bleek uit een rapport over *spyware*.<sup>26</sup> *Spyware* is vrijelijk verkrijgbaar op de consumentenmarkt, via Amazon, Bol en speciale *spyshops*. Denk daarbij aan infraroodcamera's waarmee je de activiteiten in de slaapkamer van de burens kan bekijken, pennen die met een klik zijn om te toveren tot opname-apparaat en spionagesoftware die expliciet wordt aangeprezen om je partner of werknemer mee te bespieden en waarmee je alle mails, locatiegegevens, apps en foto's van iemands telefoon kan lezen en je de camera en microfoon van die telefoon op afstand kan inschakelen om zo mee te luisteren en kijken in de ruimte waar diegene zich bevindt. Natuurlijk zijn zelfs voor deze producten bonafide toepassingen te bedenken: middels een infraroodcamera kijken of er een steenmarter in de spouwmuur zit, een journalist die in een undercoveroperatie zijn microfoon gebruikt, een partner die zijn wederhelft na een misstap toestemming geeft alle activiteiten op de telefoon te monitoren. Maar die toepassingen zijn sterk in de minderheid.

Een optie die uit het rapport volgde was dan ook dat bepaalde technieken zouden kunnen worden verboden. Daar wil de regering echter principieel niet aan.

'Ten aanzien van de in het onderzoek voorgestelde verbodsbepalingen stel ik voorop dat – op Europees noch nationaal niveau – niet snel wordt overgegaan tot verbodsbepalingen op apparaten, gezien het belang vanuit vrije marktwerking. Een verbod kan worden overwogen wanneer dat nodig zou zijn ter bescherming van de openbare orde of de openbare veiligheid, of als daarmee een zwaarwegend maatschappelijk belang is gediend. Dan zal bovendien moeten zijn gebleken dat er geen minder zwaarwegende alternatieven voorhanden zijn. Op dat punt verkeren we op dit moment niet met de in het onderzoeksrapport gemeld[e] producten. Het gaat om producten die geen illegaal gebruiksdoel hebben en waarvan het enkele bezit of gebruik nog geen inbreuk veroorzaakt op de rechtsorde of de gerechtvaardigde belangen van derden. Wanneer een bezitter te kwader trouw is, en het product wordt gebruikt als hulpmiddel om een strafbaar feit te plegen, kan het uit het verkeer worden genomen door bijvoorbeeld inbeslagneming en verbeurdverklaring. Voor algehele verbodsbepalingen ontbreekt naar het oordeel van ik [sic] derhalve de noodzaak.'<sup>27</sup>

Zelfs als een techniek in de praktijk bijna altijd wordt gebruikt voor malafide doeleinden, dan zijn restricties in de regeringsvisie onwenselijk als daarmee ook (een minimaal aantal) bonafide toepassingen onmogelijk worden gemaakt.

Zelfs bij het advies om volledige geautomatiseerde autonome wapensystemen, in de volksmond ook wel *killer drones* genoemd, die per definitie niet aan het internationale recht voldoen omdat ze zonder menselijk tussenkomst besluiten nemen met aanmerkelijke gevolgen, te verbieden,<sup>28</sup> plaatste de regering tal van kanttekeningen. Het wilde zich weliswaar inspannen om in internationaal verband te streven naar een verbod, maar meende dat daarbij wel van belang was 'oog te hebben voor het complexe internationale krachtenveld. De definitie en afbakening van een verbod luistert nauw. Voor het kabinet is het kerndoel van een verbod het behoud van het oordeelsvermogen van de mens bij inzet van een wapensysteem. Het is dan ook van belang om een algemeen onderscheid te maken tussen autonome wapensystemen die wel conform het bestaande internationale recht kunnen worden ontwikkeld en ingezet, en autonome wapensystemen waarbij dat niet mogelijk is. Er moet gewaakt worden voor een te ruime definitie zodat bestaande systemen die belangrijk

**Zelfs als een techniek in de praktijk bijna altijd wordt gebruikt voor malafide doeleinden, dan zijn restricties in de regeringsvisie onwenselijk als daarmee ook bonafide toepassing onmogelijk worden gemaakt**

zijn voor onze nationale veiligheid, zoals de Goalkeeper en de Patriot, niet onder het verbod zouden kunnen vallen. Een te krappe definitie zou er in de praktijk toe kunnen leiden dat het verbod weinig effect heeft. Voor de haalbaarheid en effectiviteit van het verbod is het tevens van belang dat de staten die actief zijn op het gebied van de ontwikkeling van autonome wapensystemen zich daarbij aansluiten. Ook moet Defensie samen met bondgenoten onderzoek kunnen doen naar volledige autonome wapensystemen die in gebruik kunnen zijn of worden genomen door potentiële tegenstanders. Defensie moet kennis hebben van de systemen van potentiële tegenstanders, ook als dat volledig autonome wapensystemen zijn die niet verenigbaar zijn met het internationale recht.<sup>29</sup>

### 3. Techno-optimisme

Alhoewel iedere specifieke digitale technologie in deze benadering als zodanig als neutraal wordt gezien – in de zin dat die voor zowel goede als slechte doeleinden kan worden ingezet – hebben de digitalisering en dataficatie van de samenleving in de regeringsvisie in het algemeen een positief en wenselijk effect. Het kerndoel van het techniekbeleid is dan ook de randvoorwaarden van technologische vooruitgang scheppen; een beleid waarin excessen worden tegengaan en technologische innovatie voor de rest zijn gang kan gaan en zelfs wordt gestimuleerd. De overheid investeert flink in innovatie en faciliteert de inzet van technieken door het creëren van labs en proeftuinen.

Toch zijn er signalen dat de verwachtingen waarmee een techniek aanvankelijk wordt geïntroduceerd uiteindelijk niet worden gerealiseerd. De toeslagenaffaire kent zijn oorsprong bijvoorbeeld in de keuze om duizenden belastingambtenaren te ontslaan en in plaats daarvan een klein aantal data-analisten in te schakelen; het proces zou met algoritmen veel beter, effectiever en rechtvaardiger kunnen worden gemaakt. Het Systeem RisicoIndicatie lijkt niet tot de opsporing van enig fraudegeval te hebben geleid; experimenten met *predictive policing* hebben geen positief effect op de criminaliteitscijfers laten zien.<sup>30</sup> De WRR waarschuwde in een recent rapport dan ook voor al te hooggespannen verwachtingen en haar eerste aanbeveling was om het beeld rond technologie te demystificeren.<sup>31</sup> In een reactie benadrukt de regering echter wederom het grote economisch en maatschappelijk belang van technologie en wijst daarbij op de bijzondere voordelen van AI:

‘Het AI-beleid draait om het vergroten van vertrouwen in AI-systemen en het optimaliseren van kansen. AI als technologie ondersteunt ook onze welvaart, de borging van publieke waarden en draagt bij aan het oplossen van maatschappelijke vraagstukken.’<sup>32</sup>

Als de regering al wetgeving aanneemt binnen het digitale domein dan is dat doorgaans om meer gegevensverwerking of de toepassing van een nieuwe technologie door bijvoorbeeld de politie, inlichtingendiensten of de belastingdienst mogelijk te maken. Uit de memories van toelichting en de antwoorden op Kamervragen blijkt dat zij dat doet uit de overtuiging dat dit processen effectiever en efficiënter zal maken, zonder dat de overtuiging wordt gestaafd met bewijs. Dat bewijs kan soms ook niet worden geleverd, omdat een techniek nog in de kinderschoenen staat. Daarom heeft zowel een WRR<sup>33</sup> als een WODC<sup>34</sup> rapport voorgesteld om de inzet van technologie dan in ieder geval achteraf te toetsen, door van tevoren een nulmeting te doen, benchmarks te formuleren en na een jaar of twee jaar te bezien in hoeverre de verwachte voordelen van de inzet van technologie ook daadwerkelijk zijn geëffectueerd. In die gedachte is de regering echter niet meegegaan, zodat haar techno-optimisme moeilijk falsifieerbaar is.

### 4. Kool en geit sparen

Alhoewel er in de regeringsvisie grote aandacht is voor de vermeende intrinsieke voordelen van technologie en digitalisering, geldt dat niet in dezelfde mate voor de intrinsieke nadelen. Eigen aan data-gedreven werken is bijvoorbeeld dat op basis van historische data patronen worden gedestilleerd en daarmee toekomstvoorspellingen worden gedaan. Als die worden gebruikt om overheidshandelen te sturen, dan leidt dat bijna automatisch tot een herbevestiging van bestaande structuren, ook van maatschappelijke ongelijkheid. Intrinsiek aan algoritmisch werken is ook dat niet wordt gekeken naar de individuele burger en de omstandigheden van het geval, maar naar de burger als onderdeel van een groep. Als 80% van de inwoners van een wijk fraudegevoelig is, dan wordt dat gebruikt als relevante informatie als een nieuw persoon in die wijk komt wonen. Dat is niet een bijeffect van algoritmische besluitvorming; de efficiëntievoordelen van algoritmische besluitvorming komen juist voort uit het feit dat mensen niet meer als individu op basis van hun particuliere

26. M. Galic et al. (2020), *Spioneren met hobbydrones en andere technologieën door burgers*, WODC-rapport 3063, repository.wodc.nl/handle/20.500.12832/2473.

27. Kamerstukken II 2020/21, 34926, nr. 11.

28. G.J. Broeks et al. (2021), *Autonome wapensystemen: het belang van reguleren en investeren*, AIV-advies 119, CAVV-advies 38 3 december 2021, adviesraadinternationalevraagstukken.nl/binaries/adviesraadinternationalevraagstukken/documenten/publicaties/2021/12/03/

autonome-wapensystemen/Autonome\_Wapensystemen\_AIV-advies\_119\_210312.pdf.

29. Kamerstukken II 2021/22, 35925-X, nr. 90.

30. B. Mali, C. Bronkhorst-Giesen & M. Den Hengst (2017), *Predictive policing: lessen voor de toekomst. Een evaluatie van de landelijke pilot*, Politieacademie, februari 2017, politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/93263.pdf.

31. WRR, *Opgave AI. De nieuwe systeemtechnologie*, rapport nr. 105, 2021, wrr.nl/

publicaties/rapporten/2021/11/11/opgave-ai-de-nieuwe-systeemtechnologie.

32. Kamerbrief met kabinetsreactie op WRR-rapport ‘Opgave AI: de nieuwe systeemtechnologie’ d.d. 7 oktober 2022, Kamerstukken II 2022/23, 26643, nr. 943.

33. WRR, *Big Data in een vrije en veilige samenleving*, rapport nr. 95, 2016, wrr.nl/adviesprojecten/big-data-privacy-en-veiligheid/documenten/rapporten/2016/04/28/big-data-in-een-vrije-en-veilige-samenleving.

34. B. van der Sloot & S. van Schendel

(2019), *De Modernisering van het Nederlands Procesrecht in het licht van Big Data. Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving*, TILT/WODC, Tilburg, WODC-rapport 2900 repository.wodc.nl/handle/20.500.12832/2390.

## Als technologische ontwikkelingen rechtsstatelijke beginselen ondergraven kiest de regering er voor om zowel de kool als de geit te sparen

omstandigheden en kenmerken worden beoordeeld. Dit soort vraagstukken lijken vooralsnog een blinde vlek in het regeringsbeleid.

Als technologische ontwikkelingen rechtsstatelijke beginselen ondergraven kiest de regering er voor om zowel de kool als de geit te sparen: technologische vooruitgang wordt aangemoedigd en het vigerende juridische kader wordt in stand gelaten, zonder dat duidelijk wordt gemaakt hoe die twee zich tot elkaar verhouden.<sup>35</sup> Ook als een voor de analoge wereld ontwikkeld rechtsbeginsel moeilijk aansluit op de digitale realiteit laat de regering de doctrine doorgaans intact, zonder aanvulling of verdere toevoeging. Zo is het discriminatierecht gestoeld op een aantal beschermde gronden, kenmerken op basis waarvan mensen vaak discrimineren (ras, gaardheid, sekse). Algoritmes maken ook onderscheid, maar dat gebeurt niet per se op deze gronden. Ras kan een even voorspellende waarde hebben als inkomen op de vraag hoeveel Marmite iemand eet. De vraag is dus of het in het kader van algoritmische besluitvorming überhaupt zinnig is om met beschermde gronden te werken en zo ja, of die lijst niet moet worden aangepast. Ook speelt dat alle data indirect correleren aan de beschermde gronden. Van de personen die een bepaalde shampoo kopen is bijvoorbeeld 84% vrouw, van boven de 50 en heeft 13% een Surinaamse achtergrond. Indirect zegt alles iets over alles. Daarbij komt dat het discriminatierecht primair kijkt naar het uiteindelijke besluit dat wordt genomen, terwijl bij algoritmische besluitvorming het meeste fout gaat in de voorfase: welke data verzamel je, hoe verzamel en label je die, hoe richt je het algoritme in, door wie worden de resultaten geïnterpreteerd, etc. Daarover zegt het recht weinig.

Dit zijn slechts enkele van de knelpunten die werden signaleerd in een BZK-rapport.<sup>36</sup> De regering ging daar in haar reactie echter niet op in,<sup>37</sup> met één uitzondering, namelijk het probleem dat door een beperking op de verwerking van gevoelige persoonsgegevens discriminatieproblemen lastig kunnen worden vastgesteld (het is moeilijk om te beoordelen of een algoritme discrimineert op basis van ras als de etnische afkomst van personen onbekend is).

‘Het kabinet zal een additionele wettelijke grondslag voor de verwerking van bijzondere persoonsgegevens in het leven roepen die ertoe strekt het onder strenge voorwaarden mogelijk te maken gegevens te verwerken om discriminatie in een algoritmisch model te voorkomen.’<sup>38</sup>

De wetswijziging maakt dus meer dataverwerking mogelijk en sluit aan bij het idee dat dataverwerking moet worden gefaciliteerd (pijler 3).

### 5. Ex post regulering

In het bestaande juridische kader is vrijwel uitsluitend gekozen voor *ex post*-regulering. De regering heeft een voorkeur voor dit reguleringstype omdat *ex ante*-regels ook legitieme toepassingen onmogelijk maken en daarmee een remmend effect hebben op digitale innovatie (pijler 2). Deze keuze heeft echter een belangrijk gevolg: het is de (mede)oorzaak van het grootste knelpunt in het digitale domein, namelijk het toezicht op en de handhaving van het juridisch kader. *Ex post*-regulering zorgt ervoor dat de verzameling, verwerking en publicatie van informatie pas achteraf kan worden beoordeeld. Daarbij speelt dat steeds meer alledaagse producten burgers, bedrijven en overheden in staat stellen data van anderen te verzamelen en te verspreiden. De enorme hoeveelheid data (denk alleen al aan het aantal foto's en video's dat per dag op Instagram, Facebook en TikTok verschijnt) die worden geüpload maakt adequate controle daarop door de Autoriteit Persoonsgegevens of politie vrijwel onmogelijk.

Dat brengt een aantal zaken met zich. Ten eerste dat hun aandacht en energie vrijwel uitsluitend uitgaan naar een handvol extremere schendingen (vaak relaterend aan de lichamelijke privacy en evidente vormen van discriminatie), maar dat het overgrote deel van vervelende, maar niet acuut problematische rechtsschendingen ongemoeid wordt gelaten. Dit zorgt voor een normalisering van deze kleine rechtsschendingen. Ten tweede dat een rechtsschending reeds heeft plaatsgegrepen en de schade is aangedaan als er eenmaal juridisch wordt opgetreden. Het achteraf verhalen van schade is vaak lastig en als het al tot een veroordeling leidt, krijgt het slachtoffer van bijvoorbeeld wraakporno vaak slechts enkele honderden of duizenden euro's toegekend, terwijl de publicatie daarvan iemand voor het leven kan tekenen.<sup>39</sup>

Uit een serie rapporten omtrent horizontale privacy (privacy tussen burgers onderling),<sup>40</sup> volgt dan ook steeds dezelfde conclusie. Het materiële recht verbiedt reeds de meeste kwalijke kanten van technologieën, maar die verboden zijn in de praktijk niet of nauwelijks te handhaven. Ten aanzien van het gebruik van drones en spionageproducten werd bijvoorbeeld geconcludeerd dat ‘het grootste euvel ten aanzien van drones en spionageproducten niet zozeer is gelegen in juridische lacunes en onduidelijkheden [...], maar in een gebrek aan naleving en handhaving van de bestaande regels.’<sup>41</sup> Dezelfde conclusie volgde uit een rechtsvergelijkend onderzoek naar horizontale privacy,<sup>42</sup> uit een studie naar *facial recognition*<sup>43</sup> en uit een onderzoek naar *deepfakes*.<sup>44</sup> Wil de regering iets doen aan dit probleem, zo was de conclusie in elk van deze rapporten, dan zal het moeten kijken naar het procesrecht, de uitbereiding van de handhavingcapaciteit en de introductie van *ex ante*-regels (denk naast verboden op techniek bijvoorbeeld aan certificering van verkooppunten, controle op kopers of het stellen van technische randvoorwaarden aan productontwikkeling).

De regering is echter zeer terughoudend op dit punt, met een opmerkelijke uitzondering: het heeft een bijna heilig geloof in *impact assessments*. Het is duidelijk waarom deze *ex ante*-maatregel de uitzondering op de regel vormt: zulke assessments hebben niet het effect dat technologische innovatie wordt beperkt, maar ten doel de kansen en risico's van een specifieke toepassing van techniek

in kaart te brengen, om vervolgens de gevaren te mitigeren en de kansen te optimaliseren voordat de techniek in gebruik wordt genomen. Zo dient de Impact Assessment Mensenrechten en Algoritmes als hulpmiddel om te identificeren of het in te zetten algoritme grondrechten zal raken; zo ja, dan maakt het een gestructureerde discussie mogelijk over de vraag of er mogelijkheden zijn om deze grondrechtenaantasting te voorkomen of te mitigeren, en of er gronden zijn waarom de (al dan niet gemitigeerde) grondrechtenaantasting toch aanvaardbaar moet worden gevonden.<sup>45</sup> De impact assessment sluit dus aan bij het idee van techniek als neutraal middel dat goede en slechte kanten kent (pijler 2) en de wens om toepassing van techniek zo veel mogelijk te faciliteren (pijler 3).

## 6. Individuele belangen

De regering richt zich in discussies over techniek met name op de bescherming van individuele belangen, wat deels volgt uit de keuze voor *ex post*-regulering (pijler 5) en het geloof in techniekneutraliteit (pijler 2). Als een bepaalde digitale technologie als zodanig een onwenselijke maatschappelijke impact heeft, dan ligt *ex ante*-regulering voor de hand. Als de regering bijvoorbeeld van mening zou zijn dat *deepfake*-technologie als zodanig schadelijk voor de samenleving is, omdat het aan het *post truth*-tijdperk bijdraagt en omdat 96% van alle *deepfakes fake-porno* betreft, dan ligt een geheel of gedeeltelijk verbod voor de hand. In *ex post*-regulering wordt daarentegen een specifieke toepassing beoordeeld; daarmee gaat de aandacht primair uit naar de particuliere belangen van een of enkele rechtssubjecten, bijvoorbeeld van de vrouw die in een specifieke *deepfake* wordt geportretteerd, en niet naar de impact van de technologie als zodanig op de maatschappelijke positie van vrouwen.

In het huidige recht ligt de nadruk dan ook primair op individuele rechtsbescherming van slachtoffers en belanghebbenden in specifieke gevallen, een benadering die goed werkt voor veel traditionele rechtsgeschillen: een bouwvergunning die wordt afgewezen, een verzoek om schadevergoeding na een lasterlijke publicatie of een beperking van privacy door de overheid, waarbij iemands telefoon voor een bepaalde periode wordt afgetapt. Steeds is de mogelijke inbreuk beperkt tot een specifiek persoon of een kleine groep, is de eventuele schending in tijd en ruimte af te bakenen en is het belang dat op het spel staat individueel en duidelijke bepaalbaar. Het is daarom

logisch dat de regering deze benadering extrapoleert naar het digitale domein; ook daar werkt het goed voor veel specifieke incidenten. Toch spelen daar ook andersoortige vraagstukken die vanuit deze benadering lastig te adresseren zijn.

*Big data*-projecten zijn bijvoorbeeld nauwelijks in tijd, ruimte en persoon af te bakenen, maar vormen een structureel en voortdurend onderdeel van de handelingen en gedragingen van overheidsdiensten, bedrijven en burgers. De camera's op de hoek van vrijwel iedere straat in de grote steden hebben bijvoorbeeld geen specifiek effect op één bepaald individu, ze filmen permanent eenieder die zich in de stad begeeft; een inlichtingendienst die de communicatiegegevens van een hele wijk of een stad verzamelt raakt niemand specifiek of individueel, maar iedereen gelijkmatig; de politie die door gebruikmaking van *predictive policing* in bepaalde wijken meer surveilleert dan in andere brengt daarmee geen schade toe aan concrete individuen. Het kan zo zijn dat de data en het algoritme dat de politie gebruikt *biased* zijn en de politie in onevenredige mate naar wijken wordt gestuurd waar veel mensen met een migratieachtergrond wonen. Als de politie vervolgens echter alleen mensen arresteert waartegen een redelijke verdenking geldt, dan is er in het particuliere geval geen onrecht gedaan; toch is een *biased* politiezet niet in het algemeen belang.

Dit soort meer systemische gevolgen van data-gedreven projecten en de problemen die zich 'onder de motor' bevinden zijn lastig te adresseren middels het huidige juridische kader. In lijn met de geachte dat het recht om de borging van individuele belangen gaat, terwijl een discussie over het algemene belang thuishoort bij de politiek, en vanuit het uitgangspunt geen problemen op te lossen die zich nog niet hebben gemanifesteerd (een *biased* database hoeft niet per se tot onwenselijk beleid te leiden) wijst de regering voorstellen om deze nieuwe vraagstukken juridische te adresseren grotendeels van de hand.<sup>46</sup>

## 7. Individuele controle

Uit de nadruk op de bescherming van individuele belangen volgt een nadruk op individuele controle en subjectieve rechten. Het is met name aan burgers om in het geval er in hun particuliere geval een rechtsschending heeft plaatsgegrepen (de buurman die met een minidrone door het keukenraampje vliegt, een lasterlijke uitspraak op

35. B. van der Sloot & E. Keymolen, 'Happy city, of een nieuwe grondwet voor de 21ste eeuw', in: J. Goossens et al. (eds), *Rechtsvorming in een hypercomplexe samenleving: Bundel n.a.v. de Staatsrechtconferentie 2022* (Tilburg University), Wolf Legal Publishers (WLP) 2022.

36. B. van der Sloot et al., *Non-discriminatie by design* (2021), digitaleoverheid.nl/nieuws/handreiking-voor-ontwikkeling-niet-discriminerende-ai/.

37. In plaats daarvan verwees ze naar de bijbehorende handreiking waarin is getracht het bestaande kader om te katten naar de

algoritmische context: B. van der Sloot et al. (2021), *Handreiking non-discriminatie by design*, <https://open.overheid.nl/repository/r/nl-3f9fa69c-acf4-444d-96e1-5c48df00eb3c/1/pdf/bijlage-1-handreiking-non-discriminatie-by-design.pdf>.

38. *Kamerstukken II* 2020/21, 26643, nr. 765.

39. Daarbij komt het Barbra Streisand-effect: [bbc.com/news/uk-18458567](https://www.bbc.com/news/uk-18458567).

40. *Kamerstukken II* 2017/18, 34926, nr. 2.

41. M. Galic et al. (2020), *Spioneren met hobbydrones en andere technologieën door burgers*, WODC-rapport 3063,

[repository.wodc.nl/handle/20.500.12832/2473](https://repository.wodc.nl/handle/20.500.12832/2473).

42. B. Schermer & B. van der Sloot (2020), *Het recht op privacy in horizontale verhoudingen*, WODC-rapport 3062, repository.wodc.nl/handle/20.500.12832/2472.

43. E. Keymolen et al. (2020), *Op het eerste gezicht*, WODC-rapport 2992, repository.wodc.nl/handle/20.500.12832/2439.

44. B. van der Sloot, Y. Wagenveld & B.J. Koops (2021), *Deepfakes*, WODC-rapport 3137, repository.wodc.nl/handle/20.500.12832/3134.

45. J. Gerards et al. (2021), *Impact Assess-*

*ment Mensenrechten en Algoritmes*, [rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2021/02/25/impact-assessment-mensenrechten-en-algoritmes/IAMA.pdf](https://rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2021/02/25/impact-assessment-mensenrechten-en-algoritmes/IAMA.pdf).

46. *Kamerstukken II* 2020/21, 26643, nr. 726, Bijlage 2: *Reactie op de afzonderlijke reguleringsopties in het rapport 'Modernisering procesrecht in het licht van big data'*.

## Terwijl er op andere terreinen afscheid wordt genomen van een eenzijdige nadruk op individuele controle en verantwoordelijkheid, houdt de regering hier juist binnen het digitale domein aan vast

Facebook, de belastingdienst die een discriminatoir besluit neemt), hun recht te halen door een klacht in te dienen en eventueel naar de rechter te stappen. Deze benadering komt voort uit het beeld van de mens als *homo economicus*: als de burger voldoende informatie en controlemogelijkheden heeft, dan is hij in principe het best gepositioneerd om zijn eigen belangen te behartigen. Overheidsingrijpen voelt in deze visie al snel als paternalistisch en beperkend.

De informatiele zelfbeschikking is dan ook het belangrijkste anker van het Nederlandse techniekbeleid. Alleen al in het kader van horizontale privacy is de regering van zins een publiekscampagne te starten die burgers bewust moet maken van de privacyrisico's van digitale applicaties, de AP te vragen het MKB beter voor te lichten, door middel van de AVG helpdesk zorg- en sportinstellingen voor te lichten, middels het project 'Maatschappelijke Dialoog' burgers, ondernemers en overheden bij elkaar te brengen, de ECP te vragen een Privacywijzer te ontwikkelen, een juridisch steunpunt op te zetten en een campagne 'Denk 2x na voordat je iets deelt' te lanceren.<sup>47</sup> Daarnaast wil het kabinet primair inzetten op het vergroten van de controlemogelijkheden van het individu.

'Elke burger moet zijn eigen gegevens bij de overheid en bedrijven zoveel mogelijk kunnen inzien, corrigeren en hergebruiken. Bovendien moet je zelf kunnen bepalen met wie je deze gegevens deelt zonder dat er iemand over je schouders mee kijkt.'<sup>48</sup>

Dat heet de regierol van de burger.

Deze benadering was lange tijd beleidsbreed dominant zowel in Nederland specifiek als in de westerse wereld in het algemeen. Denk aan slogans als 'een beter milieu begint bij jezelf', 'ieder pondje gaat door het mondje' of 'een slimme meid is op de toekomst voorbereid'. Steeds is het individu primair verantwoordelijk voor een meer algemeen maatschappelijk probleem. Langzamerhand begint daar verandering in te komen. Natuurlijk moeten kinderen leren gezonde keuzes te maken, maar het helpt niet als de schoolkantine alleen vette snacks aanbiedt; natuurlijk moeten mensen zuinig omgaan met energie, maar het milieuprobleem zal niet verdwijnen als iedere burger een spaarlamp indraait; natuurlijk is het goed als iedereen zelf alert is op specifieke vormen van discriminatie, maar er ligt ook een taak bij de overheid om systemisch racisme tegen te gaan.

Als ergens de grenzen van individuele controle duidelijk worden is het binnen het digitale domein. Individu- en weten vaak niet dat er gegevens over hen worden

verzameld en verwerkt (o.a. door cookies, geheime monitoring en *ambient technologies*). Zelfs als een burger zich wel bewust is van het feit dat zijn gegevens worden verwerkt, dan nog is het bijna onmogelijk om van de naar schatting enkele duizenden partijen die persoonsgegevens over hem verwerken na te gaan waarom en hoe zij dat doen, te controleren of dat in overeenstemming met de wet gebeurt en zo niet, daar een juridische zaak van te maken. Daarbij komt dat de technologische processen (*deep learning*, *mass surveillance*, algoritmische besluitvorming) vaak ongelofelijk complex zijn en de kosten van een rechtszaak significant zijn terwijl de burger doorgaans tegenover een overheidsorganisatie of internetonderneming staat die over grote technische kennis beschikt en de tijd en middelen heeft om lange juridische procedures uit te vechten.

Het is daarom opvallend dat terwijl er op andere terreinen afscheid wordt genomen van een eenzijdige nadruk op individuele controle en verantwoordelijkheid, onder meer naar aanleiding van een kritisch rapport van de WRR,<sup>49</sup> de regering hier juist binnen het digitale domein aan vasthoudt. Omdat ze geen verklaring geeft waarom het digitale domein de uitzondering op de regel zou zijn of voor welk probleem het vergroten van de informatiele zelfbeschikking een oplossing is (komen de knelpunten in het digitale domein voort uit een gebrek aan individuele datacontrole?) lijkt het regeringsbeleid ook op dit punt primair te zijn gestoeld op een ideologische overtuiging, namelijk aangaande de juiste rolverdeling tussen burger en overheid.

### 8. Europees beleid

Wat vervolgens opvalt is dat enkele marginale wetswijzigingen daargelaten, vrijwel alle regelgevende kaders binnen het digitale domein uit Europa afkomstig zijn. Zo heeft het Europees Hof voor de Rechten van de Mens een uitgebreid raamwerk ontwikkeld voor dataverwerking door inlichtingendiensten<sup>50</sup> en is de Europese Unie met een groot aantal wetgevingstrajecten gekomen. Na de afronding van de AVG<sup>51</sup> en de Politierichtlijn<sup>52</sup> is er onder meer gewerkt aan de AI Act,<sup>53</sup> de Digital Markets Act,<sup>54</sup> de Digital Services Act,<sup>55</sup> de e-Privacy Regulation,<sup>56</sup> de Open Data Directive,<sup>57</sup> de Data Act<sup>58</sup> en de Data Governance Act.<sup>59</sup> Typisch aan de Nederlandse houding is dat er vervolgens vrij weinig invulling wordt gegeven aan de Europese regels, terwijl die daartoe wel de ruimte laten of zelfs expliciet aanmoedigen.

Een voorbeeld is de AVG, die een algemeen kader geeft en die van Lidstaten vraagt daar door middel van een uitvoeringswet (UAVG) verder handen en voeten aan te geven. Nederland maakt echter nauwelijks gebruik van deze mogelijkheid, zo bleek uit recent onderzoek.



'Het onderzoek maakt duidelijk dat de UAVG eigenlijk maar een beperkte betekenis heeft. Duidelijk is in ieder geval dat de wet geen nadere invulling biedt aan de AVG normen. Dat is wellicht begrijpelijk gelet op de ontstaansgeschiedenis van de UAVG, de beperkte tijd die voor de totstandkoming beschikbaar was en de keuze voor een 'beleidsneutrale' omzetting van de bestaande normen die destijds is gemaakt. Maar daarmee is de toegevoegde waarde van de UAVG slechts beperkt. En dat kan worden betreurd nu de in de AVG neergelegde normen voor velen lastig te hanteren zijn.'<sup>60</sup>

De regering erkent wel de noodzaak tot verdere concretisering van regels, maar wijst daarbij doorgaans naar anderen: de EU, rechters, de Autoriteit Persoonsgegevens. Een voorbeeld is de reactie van de Minister van Rechtsbescherming op de discussie omtrent de rol van internetplatformen.

'Voor mij staat als een paal boven water dat het niet zo kan zijn dat platformen eigen regels hanteren die ruimte bieden aan strafbare of anderszins onrechtmatige uitingen op het internet. Daartegenover geldt dat platformen weliswaar het recht hebben zelf te bepalen of zij bepaalde vormen van content willen weigeren die noch strafbaar, noch anderszins onrechtmatig is (bijvoorbeeld consensuele naaktheelden), maar dat daarbij wel steeds aandacht moet zijn dat de vrijheid van meningsuiting niet onnodig wordt beperkt. Bij onrechtmatige uitingen is het toetsingskader veelal de onrechtmatige daad (artikel 6:162 BW), dan wel het bestuursrecht. Het kan niet van platformen verlangd worden dat zij steeds de

juiste afwegingen maken in het vaststellen of een uiting al dan niet onrechtmatig is. Naar mijn mening van het kabinet ligt er een taak bij de AP om via haar oordelen een standaard te ontwikkelen voor rechtmatige online content. Ik zal met de AP in gesprek gaan en in beeld brengen wat er nodig is om de AP invulling te laten geven aan deze taak.'<sup>61</sup>

De Autoriteit Persoonsgegevens heeft vooralsnog echter weinig verdere invulling gegeven aan de abstracte noties uit de AVG, wat ook geldt voor het Europese samenwerkingscollectief van handhavende organisaties: de European Data Protection Board. De hoop dat de invulling van het algemene kader per sector zou worden vormgegeven door gedragscodes blijkt vooralsnog ijdel te zijn geweest. Er zijn ruim zes jaar na het aannemen van de AVG in heel Europa slechts zes gedragscodes goedgekeurd.<sup>62</sup> Het gevolg daarvan is dat als er al meer duidelijkheid wordt geboden omtrent de precieze interpretatie en implementatie van de regels per context, dit van rechters moet komen. Enkele uitzonderingen daargelaten spelen de meeste rechtszaken binnen de digitale sfeer zich echter op eerste aanleg- en kort geding-niveau af, zodat rechtspraak vrij versplinterd blijft. Bovendien werkt een systeem van algemene regels die vervolgens worden uitgekristalliseerd in de rechtspraak doorgaans alleen bij een vitale procescultuur, terwijl burgers in de digitale sfeer juist machteloos staan tegen grote dataverwerkende organisaties en dus doorgaans afzien van een juridische procedure (pijler 7).

## 9. Algemene regels

Het gevolg van de keuze om het in grote lijnen bij het Europese kader te laten (pijler 8) is dat de regels in de

47. Kamerstukken II 2018/19, 34926, nr. 8 en Kamerstukken II 2020/21, 34926, nr.

11. [twitter.com/i/status/1456546145124093952](https://twitter.com/i/status/1456546145124093952) en

[veiliginternetten.nl/denkvoorjedeelt/](https://veiliginternetten.nl/denkvoorjedeelt/).

48. *Werkagenda Waardengedreven Digitaliseren*, bijlage bij Kamerstukken II 2022/23, 26643, nr. 940.

49. WRR, *Weten is nog geen Doen*, rapport nr. 97, 2017, [wrr.nl/publicaties/rapporten/2017/04/24/weten-is-nog-geen-doen](https://wrr.nl/publicaties/rapporten/2017/04/24/weten-is-nog-geen-doen).

50. [echr.coe.int/documents/fs\\_mass\\_surveillance\\_eng.pdf](https://echr.coe.int/documents/fs_mass_surveillance_eng.pdf).

51. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [eur-lex.europa.eu/eli/reg/2016/679/oj](https://eur-lex.europa.eu/eli/reg/2016/679/oj).

52. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for

the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, [eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680).

53. Proposal for a Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts Com/2021/206 Final, [eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206).

54. Proposal for a Regulation Of The European Parliament And Of The Council on contestable and fair markets in the digital sector (Digital Markets Act) COM/2020/842 final, [eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN](https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN).

55. Proposal for a Regulation Of The European Parliament And Of The Council on a Single Market For Digital Services (Digital

Services Act) and amending Directive 2000/31/EC COM/2020/825 final, [eur-lex.europa.eu/legal-content/en/ALL/?uri=COM:2020:825:FIN](https://eur-lex.europa.eu/legal-content/en/ALL/?uri=COM:2020:825:FIN).

56. Proposal for A Regulation Of The European Parliament And Of The Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final - 2017/03 (COD), [eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010).

57. Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast) PE/28/2019/REV/1, [eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L1024](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L1024).

58. Proposal for a Regulation Of The European Parliament And Of The Council on harmonised rules on fair access to and use of data (Data Act) COM/2022/68 final, [eur-lex.europa.eu/legal-content/EN/](https://eur-lex.europa.eu/legal-content/EN/)

[TXT/?uri=COM%3A2022%3A68%3AFIN](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN).

59. Proposal for a Regulation Of The European Parliament And Of The Council on European data governance (Data Governance Act) COM/2020/767 final, [eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767).

60. H. Winter et al. (2022), *Bescherming gegeven?*, WODC-rapport 3249, repository. [wodc.nl/handle/20.500.12832/3193](https://wodc.nl/handle/20.500.12832/3193).

61. Kamerstukken II 2020/21, 34926, nr. 11.

62. Twee daarvan zijn overigens uit Nederland afkomstig, [edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011\\_en](https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_en).

digitale sfeer zeer algemeen blijven. De AVG geeft bijvoorbeeld eigenlijk alleen tamelijk voor de hand liggende principes die in feite volgen uit de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. Verzamel niet meer gegevens dan nodig zijn, formuleer een specifiek doel, verwerk gegevens niet voor projecten die onverenigbaar zijn met het oorspronkelijke doel, verwijder gegevens zodra die niet langer nodig zijn, sla gegevens veilig op, etc. In de praktijk worstelen dataverwerkende partijen echter met wat die algemene principes voor hun specifieke situatie betekenen: wanneer is een verwerkingsdoel specifiek genoeg en is een ander doel precies 'onverenigbaar' met het oorspronkelijke doel;<sup>63</sup> aan de hand van welke standaarden moet het datakwaliteitsprincipe worden getoetst; kan *multiparty computation* onder voorwaarden als anonimiseren gelden en zo ja, welke?

De regering kiest ervoor het antwoord op deze vragen aan dataverwerkende organisaties zelf te laten, vanuit de overtuiging dat zij het best gepositioneerd zijn om deze inschatting met medeneming van de specifieke omstandigheden van het geval te maken. Alhoewel deze benadering lange tijd goed heeft gewerkt, komt die steeds meer onder druk te staan. Een algemeen regime met vrij breed omschreven regels werkte goed in de jaren negentig, waarin slechts een klein aantal partijen toegang had tot grote databases en de geavanceerde verwerkingstechnieken die nodig waren om die data te analyseren. Nu is dat anders. Data en dataverwerkingstechnieken zijn gedemocratiseerd en daarmee zeer divers. Het *nudgen* van burgers in *smart cities* is onvergelijkbaar met ziekteverlofregistratie door werkgevers, het delen van klantgegevens door banken met de belastingdienst is wezenlijk anders dan het gebruik van patiëntgegevens voor *total genome analysis*, het maken van dronebeelden voor een verjaardagsfeestvideo heeft een andere aard dan een *smart-toilet* dat nauwgezet de ontlasting van de gebruiker analyseert. Toch geldt daar slechts hetzelfde algemene AVG-regime voor.

Ook waar meerdere juridische regimes spelen die niet eenduidig op elkaar aansluiten, kiest de Nederlandse regering ervoor om geen verdere duidelijkheid te verschaffen. Een voorbeeld is het geval waarin, zoals in toenemende mate gebeurt, private actoren (die onder de AVG vallen) en de politie (die onder de Politierichtlijn valt) samenwerken; omdat er verschillende voorwaarden en standaarden voor beide partijen zijn is niet altijd duidelijk in hoeverre data kunnen worden gedeeld en aan welke regime die data vervolgens onderhevig zijn. Zelfde vraagstukken spelen bij internationale consortia, waarin bijvoorbeeld een Nederlandse universiteit, met een Amerikaanse publieke instelling, een Braziliaans onderzoeksinstituut en een Zuid-Koreaans tech-bedrijf samenwerken. Hoe de verschillende regimes met elkaar in overeenstemming moeten worden gebracht wordt primair aan de organisaties zelf gelaten en aan de handhavende organisaties of de EU die hieromtrent nadere regels kunnen stellen.

Dat geldt zelfs op het punt waarop Europese raamwerken tegenstrijdig zijn en Lidstaten worden aangemoedigd meer duidelijkheid te scheppen. Zo volgt uit de Open Access Directive dat zo veel mogelijk overheidsinformatie actief openbaar moet worden gemaakt om hergebruik daarvan voor commerciële doeleinden mogelijk te maken, terwijl uit de AVG volgt dat zulke informatie in principe

niet openbaar mag worden gemaakt als die persoonsgegevens bevatten (wat doorgaans het geval zal zijn).<sup>64</sup> De Open Access Directive stelt dat die richtlijn niet afdoet aan de AVG, die op haar beurt nationale overheden de mogelijkheid biedt om in het kader van actieve openbaarmaking meer duidelijkheid te scheppen omtrent het conflict tussen openheid en geslotenheid, tussen hergebruik van overheidsinformatie voor commerciële doeleinden en het principe van doelbinding, tussen data zo maximaal mogelijk te benutten en het dataminimalisatiebeginsel. Daarvan heeft Nederland echter slechts marginaal gebruik gemaakt, zodat het aan organisaties zelf is om hieromtrent in hun specifieke geval een oordeel te vellen.<sup>65</sup> Zowel de Raad van State<sup>66</sup> als de Autoriteit Persoonsgegevens<sup>67</sup> hebben de regering dan ook opgeroepen om meer duidelijkheid te scheppen omtrent het hergebruik van persoonsgegevens.<sup>68</sup>

## 10. Kleine overheid

Tot slot investeert de overheid weinig in haar eigen kennispositie en potentieel als het gaat om digitalisering; het besteedt digitaliseringsprojecten doorgaans uit. Daarmee wordt de overheid steeds afhankelijker van de private sector en wordt de kennis-, expertise- en datakloof tussen tech-bedrijven en de overheid steeds groter. Dat heeft er onder meer toe geleid dat er een veelheid aan privaat-

## De overheid wordt steeds afhankelijker van de private sector en de kennis-, expertise- en datakloof tussen tech-bedrijven en de overheid wordt steeds groter

publieke samenwerkingen is ontstaan, bijvoorbeeld in zogenoemde *smart city*- en *living lab*-projecten. Daarin werken lokale overheden samen met bedrijven om de publieke ruimte vorm te geven, worden burgers genudged (onbewust gestuurd in hun gedrag) en wordt door middel van algoritmische analyse op preventieve politie-inzet bij 'afwijkende' gedragspatronen van datasubjecten (*aka* mensen) ingezet. Deze samenwerkingsverbanden brengen met zich dat tech-bedrijven met commerciële belangen invloed krijgen op de inrichting van de publieke ruimte, de levens van burgers en de inzet van overheidsmacht.

Het is niet voor niets dat het ongevraagde advies van de Raad van State over de effecten van de digitalisering voor de rechtsstatelijke verhoudingen opent met dit probleem.<sup>69</sup> Uit het Kamerdebat dat daarop volgde werd echter duidelijk dat het kabinet niet van zins is minder afhankelijk van private partijen te worden.<sup>70</sup> Als het gaat om de marktdominantie van private partijen terug te dringen bestaat er bij de Nederlandse regering tevens weinig animo. Terwijl de Europese Commissie, zij het met wisselend

succes, het mededingingsrecht gebruikt om op te treden tegen misbruik van macht, koppelverkoop en misleidende gebruikersvoorwaarden en in Duitsland onlangs Facebook's datagebruik in strijd werd geacht met het mededingingsrecht,<sup>71</sup> wordt deze route in Nederland nauwelijks bewandeld. Ook in de mogelijkheid, die onder meer door de European Data Protection Supervisor naar voren is gebracht,<sup>72</sup> om van overheidswege actief te interfereren op de digitale markt om opkomende bedrijven en start ups te helpen digitale alternatieven te ontwikkelen ziet de Nederlandse regering weinig, laat staan dat ze zelf een rol speelt in het ontwikkelen van bijvoorbeeld een privacyvriendelijke versie van Facebook, een Twitter-alternatief waarop minder nepnieuws wordt verspreid of een betere Tiktok waarin kinderen niet worden gediscrimineerd.

Terwijl de overheid anders dan op sommige andere markten zich binnen de digitale sector strikt aan haar primaire taak houdt, geldt dat niet voor tech-bedrijven. De door hun geleverde diensten zijn inmiddels met recht publieke voorzieningen te noemen (ook overheden zelf kunnen niet meer zonder de digitale infrastructuur zoals geleverd door Microsoft, Google en anderen), ze bepalen door privaatsamenwerkingen mede de ordening van de publieke ruimte en leggen zich in toenemende mate toe op het leveren van diensten die voorheen bij publieke of semi-publieke organisaties waren belegd. Zo leveren zij gratis internet in derdewereldlanden, starten ze digitale bibliotheken, richten ze zich op de verbetering van de gezondheidszorg, bieden ze nieuwe vormen van onderwijs aan en leveren ze gratis sociale woningen aan minima aan, in ruil voor hun data.<sup>73</sup> Lokale overheden geven vaak graag het stokje over aan deze organisaties, dan wel omwille van budgettaire redenen dan wel uit de overtuiging dat de markt publieke taken beter, effectiever en efficiënter kan uitvoeren.

Ook de burger krijgt in de digitale samenleving een bijzondere positie. Omdat burgers toegang hebben tot digitale technieken die hen in staat stellen meer eigen regie te voeren (pijler 7), geeft de overheid ook hun in toe-

## De dataficatie van de samenleving faciliteert het streven naar een kleine overheid

nemende mate verantwoordelijkheden die voorheen elders waren belegd. Zo is een van de door de regering voorgestelde oplossingen voor de door de vergrijzing veroorzaakte overbelasting op de zorg burgers middels digitale technieken aan zelf-diagnose en -medicatie te laten doen. Zelfs binnen de strafrechtelijke sfeer wordt hoe langer hoe meer gekeken naar een actieve rol van burgers (het mengen van blauw met grijs). Zo vraagt de politie burgers expliciet mee te doen met het opsporen en verhoren van potentiële wetsovertreders middels een app.<sup>74</sup> De dataficatie van de samenleving faciliteert daarmee het streven naar een kleine overheid.

### Conclusie

Vaak wordt het Nederlandse digitale-techniekbeleid afgeschilderd als ad hoc, eclecticisch en incident-gedreven. Uit een analyse van de kabinetsreacties op Kamervragen en rapporten en de beleidsinitiatieven van het afgelopen decennium komt echter een verrassend helder en consistent beeld naar voren. De digitalisering van de samenleving is wenselijk omdat het leidt tot meer welvaart, grotere veiligheid en betere zorg (pijler 3). Als technologie voor slechte toepassingen wordt ingezet moet dat worden geadresseerd (pijler 2), anderszins past de overheid terughoudendheid (pijler 1). De regels die er zijn voor de digitale sfeer komen dan ook primair uit Europa (pijler 8) en worden vervolgens zo open mogelijk gelaten, zodat het aan dataverwerkende organisaties zelf is om daar handen en voeten aan te geven (pijler 9), ook als oude juridische doctrines zich niet eenvoudig laten vertalen naar het digitale domein (pijler 4). Specifieke toepassingen van tech-

63. L. Moerel & C. Prins (2016), 'Privacy voor de homo digitalis: Proeve van een nieuw toetsingskader voor gegevensbescherming in het licht van Big Data en Internet of Things', in: *Homo Digitalis. Preadviezen Nederlandse Juristen-Vereeniging* 2016, Handelingen NJV, 146e jaargang/2016-1, Deventer: Wolters Kluwer 2016, p. 9-124, [nrv.nl/wp-content/uploads/2011/04/Preadviezen-NJV-2016.pdf](http://nrv.nl/wp-content/uploads/2011/04/Preadviezen-NJV-2016.pdf).

64. HvJ EU (Grote kamer) 22 juni 2021, Zaak C-439/19 (B.) EU:C:2021:504.

65. Wetsvoorstel houdende wijziging van de Wet hergebruik van overheidsinformatie en enkele andere wetten in verband met de implementatie van richtlijn nr. 2019/1024/EU van het Europees Parlement en de Raad van 20 juni 2019 inzake open data en het hergebruik van overheidsinformatie (Wet implementatie Open data richtlijn),

[wetgevingskalender.overheid.nl/Regeling/WGK009986](http://wetgevingskalender.overheid.nl/Regeling/WGK009986).

66. Raad van State, Advies over het wetsvoorstel implementatie Open data richtlijn, W04.22.0141/I, 24 oktober 2022, [raadvanstate.nl/actueel/nieuws/oktober/samenvatting-open-data-richtlijn/@132262/w04-22-0141/](http://raadvanstate.nl/actueel/nieuws/oktober/samenvatting-open-data-richtlijn/@132262/w04-22-0141/).

67. Autoriteit Persoonsgegevens, Advies over het concept voor het wetsvoorstel implementatie Open data richtlijn, z2022-00356, 28 juni 2022, [autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies\\_wijziging\\_wet\\_hergebruik\\_overheidsinformatie.pdf](https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_wijziging_wet_hergebruik_overheidsinformatie.pdf).

68. Juridisch gezien moeten open data en het hergebruik van overheidsinformatie volledig voldoen aan het gegevensbeschermingsrecht; het eerste is ondergeschikt aan het laatste juridische kader. Door open te laten hoe de twee raamwerken zich tot

elkaar verhouden menen veel organisaties echter dat zij een 'balans' moeten zoeken en maken zij meer data openbaar dan uit een lezing van de AVG zou volgen. De keuze om openheid te laten bestaan over de precieze verhouding van de twee raamwerken sluit daarmee aan bij pijlers 3 en 4.

69. *Kamerstukken II* 2017/18, 26643, nr. 557.

70. *Handelingen II* 2018/19, nr. 106, item 26, 10 september 2019 (debat over het rapport van de Raad van State over de digitalisering van de overheid).

71. T. Thiede & L. Herzog, *The German Facebook Antitrust Case – A Legal Opera*, 11 februari 2021, [competitionlawblog.kluwercompetitionlaw.com/2021/02/11/the-german-facebook-antitrust-case-a-legal-opera/](http://competitionlawblog.kluwercompetitionlaw.com/2021/02/11/the-german-facebook-antitrust-case-a-legal-opera/).

72. European Data Protection Supervisor, *Privacy and competitiveness in the age of*

*big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, maart 2014, [edps.europa.eu/sites/default/files/publication/14-03-26\\_competition\\_law\\_big\\_data\\_en.pdf](https://edps.europa.eu/sites/default/files/publication/14-03-26_competition_law_big_data_en.pdf).

73. [rtlnieuws.nl/tech/artikel/4648661/helmond-living-lab-brainport-smart-district-slimste-wijk-smart-home-unstadio](https://rtlnieuws.nl/tech/artikel/4648661/helmond-living-lab-brainport-smart-district-slimste-wijk-smart-home-unstadio).

74. [rtlnieuws.nl/editie/artikel/3691971/politie-laait-burger-meespelen-met-levens-echte-game-apps-een-heel-eng-idee](https://rtlnieuws.nl/editie/artikel/3691971/politie-laait-burger-meespelen-met-levens-echte-game-apps-een-heel-eng-idee); [rtlnieuws.nl/nieuws/nederland/artikel/4726101/politieagent-spelen-een-app-hoe-ver-mag-de-burger-gaan](https://rtlnieuws.nl/nieuws/nederland/artikel/4726101/politieagent-spelen-een-app-hoe-ver-mag-de-burger-gaan).

niek worden alleen achteraf op hun legitimiteit beoordeeld (pijler 5), waarbij primair wordt gekeken naar de particuliere belangen van een specifieke burger (pijler 6). De verantwoordelijkheid om op te komen tegen eventuele misstanden ligt primair bij de burger (pijler 7) en terwijl de overheid zelf zo min mogelijk interfereert op de digitale markt, stimuleert ze bedrijven en burgers andersom om te helpen bij de uitvoering van publieke taken of die in zijn geheel voor hun rekening te nemen (pijler 10).

Het beleidsbeeld dat hieruit opstijgt laat zich wellicht het best kenschetsen als libertarisch of neo-liberaal. Dat hoeft op zich niet te verbazen gezien de politieke krachtsverhoudingen gedurende het afgelopen decennium. Deze regelingshouding is dan ook niet uniek aan het digitale beleidsterrein; het is een uitvloeisel van het huidige politieke klimaat waarin op incidenten wordt gereageerd zonder dat altijd naar de onderliggende oorzaken wordt gekeken, waarin in plaats van vroegtijdig op signalen te reageren na een weloverwogen maatschappelijk debat, soms net zo lang wordt gewacht met actie tot een noodsituatie een voldoende politiek feit creëert,<sup>75</sup> waarin niet alleen visie, maar ook grotere parlementaire debatten over de inrichting van de samenleving grotendeels afwezig zijn,<sup>76</sup> waarin de overheid zoveel heeft geoutsourcet dat ze in toenemende mate afhankelijk is van private partijen, zowel voor primaire kennis als voor de uitvoering van beleid<sup>77</sup> en waarin er tal van adviesorganen zijn en rapport op rapport wordt aangevraagd zonder de adviezen over te nemen.<sup>78</sup>

Misschien nog wel zorgelijker dan deze constellatie is dat de ambtenarij zich grotendeels naar deze politieke mores lijkt te hebben gevoegd. Alhoewel nu wellicht meer dan vroeger heeft de politiek altijd een zekere mate van vluchtigheid gekend, is er altijd een invloed geweest van incidenten die in de media worden uitgemeten en hebben ministers en politici door een gebrek aan tijd en vak kennis op deelreinen vaker het formuleren van een langetermijnperspectief overgelaten aan anderen. De waarborg lag traditioneel besloten bij ambtenaren, die vaak decennia binnen ministeries op een specifiek beleidsterrein werkten en op basis van eigen kennis en uitgebreide discussies met experts beleid formuleerden waarin werd geanticipeerd op grotere maatschappelijke ontwikkelingen. Door de veelbesproken wijziging in de structuur van de Algemene Bestuurdienst is onder de snel roulerende topambtenaren van de Topmanagementgroep steeds minder inhoudelijke expertise ontstaan en een steeds grotere gerichtheid op management gekomen.<sup>79</sup> Gelukkig is die inhoudelijke vak kennis er op lager ambtelijk niveau nog wel. Zowel bij het Ministerie van BZK als J&V werkt op het terrein van digitalisering inmiddels een klein leger aan zeer goed ingevoerde experts. Toch is ook daar de roulatiesnelheid hoog en lijken ook zij veel van de bovengenoemde pijlers en de onderliggende ideologie te hebben geïnternaliseerd.<sup>80</sup> De meest gehoorde vraag bij het in ontvangst nemen van een advies of rapport is bijvoorbeeld: wie gaat er morgen dood als wij vandaag geen wetswijzigingen voorstellen? De vraag is ongetwijfeld provocatief geformuleerd om direct de ernst van de situatie scherp te krijgen; toch sluit de stelwijze naadloos aan bij een focus op concrete incidenten, op individuele in plaats van algemene belangen en klinkt er een terughoudendheid voor wetswijzigingen in door.

Om het Nederlandse digitaliseringsbeleid toekomstbestendig te maken zijn drie ontwikkelingen nodig.

Ten eerste moet het kabinet een duidelijke visie op digitale techniek ontwikkelen en daartoe een algemeen kader ontwikkelen. Daarbij moeten juist de grotere ethische en maatschappelijke vragen centraal staan. Willen we eigenlijk wel een samenleving waarin veel van de intermenselijke interactie is vervangen door interactie met robots, ook al is dat misschien efficiënter en goedkoper; willen we een samenleving waarin patronen uit het verleden bepalend worden voor besluiten over groepen en personen; willen we een samenleving waarin de meeste digitale platformen in handen zijn van commerciële bedrijven uit Amerika? Vooralsnog schuwt de regering dit soort vragen. Het is waar dat dit kabinet meer dan vorige kabinetten oog lijkt te hebben voor de grote invloed van digitale technologie, dat er voor het eerst een Staatssecretaris voor Digitalisering is en dat er zelfs in het Coalitieakkoord een aparte paragraaf is gewijd aan digitalisering. Toch is die paragraaf, die weliswaar gewag maakt van grondrechten, digibetisme en digitale veiligheid, voornamelijk vanuit economisch oogpunt geschreven, met aandacht voor het verzilveren van de kansen van digitalisering, de ambitie om een digitaal knooppunt te worden en de wens om digitale samenwerkingsverbanden te verbreden. De paragraaf staat niet voor niets in het hoofdstuk 'Welvarend Nederland'.<sup>81</sup> Ook de Kamerbrief van de staatssecretaris met de hoofdlijnen van het digitaliseringsbeleid, die invulling geeft aan de regeringsambitie op dit terrein, lijkt veel van de in dit artikel besproken pijlers te omarmen: zo moet digitalisering worden aangevraagd terwijl tegelijkertijd alle grondrechten, de democratie en de rechtsstaat moeten worden gewaarborgd (pijler 4), er wordt gesproken over de kansen en de risico's van digitale technologie (pijler 2) en er wordt ingezet op de regiefunctie van de burger (pijler 7).<sup>82</sup> Toch lijkt er een voorzichtige kentering in zicht. In de Werkagenda Waardengedreven Digitaliseren, die verdere invulling geeft aan deze hoofdlijnen, worden, zij het slechts letterlijk in steekwoorden, punten genoemd die mogelijk richting kunnen geven aan een toekomstgericht digitaliseringsbeleid: 'het loslaten van de vrijblijvendheid in de zelfregulering op het terrein van digitalisering', 'duidelijke grenzen stellen' en 'waar nodig publieke alternatieven ontwikkelen'.<sup>83</sup>

Ten tweede zou de Tweede Kamer een actievere rol moeten spelen in het agenderen van digitaliseringsvraagstukken, juist als het gaat om de lange lijn en de grotere (maatschappelijke) thema's. Er is inmiddels een vaste Kamercommissie Digitale Zaken geïnstalleerd. Die heeft zich voorgenomen om toekomstgericht over techniek te debatteren vanuit maatschappelijke en ethische principes. Een van de taken is dan ook het 'verkennen, doordenken en agenderen van huidige en toekomstige commissieoverstijgende ontwikkelingen op het gebied van digitalisering'.<sup>84</sup> Het zou goed zijn als dit in de toekomst inderdaad een kernthema wordt. Vooralsnog is de commissie echter met name druk met het reageren op al lopende EU-wetgevingstrajecten, met thema's als *quantum computing* die al in het WRR rapport uit 2016 uiteen zijn gezet en is het bezig om een kennispositie te verkrijgen op de meest basale juridische begrippen; zo heeft het twee experts gevraagd een factsheet te maken over wat eigenlijk een

‘persoonsgegevens’ is.<sup>85</sup> Het is raadzaam om bij het begin te beginnen omdat de Kamer doordat er de afgelopen jaren weinig structurele aandacht is geweest voor digitalisering een behoorlijke kennisachterstand heeft. Wel betekent het dat het vermoedelijk nog wel even zal duren voordat de commissie zowel goed zicht krijgt op wat de huidige wetgeving behelst als hoe bestaande technologieën daarop inwerken voordat ze kan toekomen aan toekomstige technologieën, de impact daarvan op de samenleving en de mogelijke noodzaak om huidige wetgeving op punten fundamenteel te herzien. Toch zijn ook hier positieve signalen. Zo is er, zij het sterk versplinterd, bij specifieke Kamerleden grote kennis op digitale deelgebieden,<sup>86</sup> en schuwt de Kamer steeds minder daadkrachtig op te treden tegen digitale misstanden, zoals onlangs bleek uit de oproep aan het kabinet om een verbod op *deep-fake*-technologie te overwegen gezien de grote maatschappelijke gevolgen.<sup>87</sup>

Tot slot zal ook binnen de ambtenarij verandering dienen te komen. Daarbij spelen globaal drie punten. Ten eerste is er een zeer grote mate van versplintering binnen het ambtenarenapparaat als het gaat om kennis en expertise over digitale technieken. Het ontbreekt aan een duurzaam interdisciplinair kennisecosysteem, aan een duidelijk mandaat, aan adequate financiering voor interdepartementaal langetermijnonderzoek en aan uitvoeringscapaciteit. Ten tweede is het probleem dat Nederland in de EU niet agendabepalend is. Terwijl de EU in snel-

## De Tweede Kamer zou ook een actievere rol moeten spelen in het agenderen van digitaliseringsvraagstukken, juist als het gaat om de lange lijn en de grotere (maatschappelijke) thema’s

treinvaart tientallen wetten aanneemt op het gebied van digitalisering blijft de Nederlandse bijdrage, anders dan die van sommige andere landen, vaak in de marge, nadat een wetsvoorstel al is gedaan. Ten derde zou ook binnen het Haagse de ambtenarij een veel proactievere rol moeten spelen. Ze zal een eigen kennispositie moeten opbouwen en de politiek vanuit die kennispositie moeten doorringen van de noodzaak om wetgeving aan te nemen die nu nog niet noodzakelijk lijkt, maar in de toekomst veel kwalijke gevolgen kan voorkomen. Ook op dit punt zijn positieve signalen waar de nemen. Zo is er binnen de ambtelijke top erkenning voor de bovenstaande knelpunten en lijkt er een brede wil om daar op korte termijn verandering in te brengen.<sup>88</sup> •

75. ‘Vluchtelingen crisis, klimaat crisis, stikstof crisis, woning crisis, jeugdzorg crisis en ga zo maar door. De ene crisis is nog niet voorbij of de volgende crisis wordt al weer aangekondigd. Maar zijn de problemen nou echt zoveel groter dan voorheen, of komt de stempel ‘crisis’ het openbaar bestuur ook goed uit? Als het crisis is, zal men immers niet zomaar beweren dat er niks gedaan hoeft te worden. Bovendien legitimeert het predicaat ‘crisis’ een ferm optreden – misschien nog wel ferner dan normaal gewenst of zelfs toegestaan zou zijn. Bij veel crisisdossiers gaat het niet om noodsituaties die ons overvallen hebben. Eerder gaat het om reguliere opgaven die simpelweg verwaarloosd zijn – doordat bij de overheid niet de wil bestond om ze aan te pakken, of omdat de overheid bij de aanpak steevast op te veel weerstand stuitte.’, Raad voor het Openbaar Bestuur, *Gezag Herwinnen. Over de gezagswaardigheid van het openbaar bestuur*, november 2022, [raadopenbaarbestuur.nl/documenten/publicaties/2022/11/10/gezag-herwinnen-over-de-gezagswaardigheid-van-het-openbaar-bestuur](https://raadopenbaarbestuur.nl/documenten/publicaties/2022/11/10/gezag-herwinnen-over-de-gezagswaardigheid-van-het-openbaar-bestuur).

76. ‘Door de focus op efficiëntie en effectiviteit zijn vragen over wat rechtvaardig is binnen het openbaar bestuur uit het zicht geraakt.’ Ibid.

77. ‘De Raad constateert binnen het open-

baar bestuur een bijna koortsachtige focus op de korte termijn, waardoor grote maatschappelijke problemen vaak oncontroleerbaar kunnen voortwoekeren. De Raad wil om die reden werk maken van het stimuleren van langetermijndenken binnen het openbaar bestuur. Bovendien is de overheid in de afgelopen decennia in gaan zetten op procesmanagement en sterk gaan leunen op ingehuurde experts en externe adviseurs, waardoor de cognitieve vaardigheden van de overheid zelf sterk achteruit zijn gegaan. De Raad wil nadenken over hoe die hersteld kunnen worden door expertise en ervaringsdeskundigheid van buiten naar binnen te halen.’ Ibid.

78. W. Derksen: ‘Er is te veel onderzoek en te weinig kennis’, in: J. Bussemaker et al. (eds.), *Wetenschap en overheidsbeleid. Een spanningsvolle relatie (essaybundel)*, p. 101-112, Boom bestuurskunde 2022.

79. M. Noordegraaf et al. (2020), *Kwaliteit van mobiliteit: De werking van de Algemene Bestuursdienst (ABD)*, rapportage, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Utrecht: USBO advies, [algemenebestuursdienst.nl/binaries/abd/documenten/publicatie/2021/01/15/kwaliteit-van-mobiliteit-samenvatting/samenvatting+Kwaliteit+van+Mobiliteit+De+werking+van+de+ABD+UU.pdf](https://algemenebestuursdienst.nl/binaries/abd/documenten/publicatie/2021/01/15/kwaliteit-van-mobiliteit-samenvatting/samenvatting+Kwaliteit+van+Mobiliteit+De+werking+van+de+ABD+UU.pdf).

80. ‘In de jaren 80 en 90 vond op basis van

deze ideeën een vermarkting van maatschappelijke instituties plaats. Publieke taken werden in een proces van privatisering gedelegeerd aan private instanties en de overheid riep zelfstandige bestuursorganen in het leven waarmee prestatiegerichte afspraken gemaakt werden. De overheid ging steeds vaker een beroep doen op externe experts en adviesbureaus. In plaats van inhoudelijke vaardigheden kwamen competenties als procesmanagement in het werk van ambtenaren centraal te staan. De nieuwe bestuurlijke rationaliteit ging gepaard met een technocratisering van het maatschappelijk debat. Niet idealen maar pragmatische oplossingen werden dominant. Het bewaken van complexe processen en het halen van targets werd een doel op zich. Bestuurders en politici grepen steeds vaker terug op wetenschappelijk onderzoekshandelen te verantwoorden en beleidsalternatieven uit te sluiten.’ Daarom acht de Raad het van groot belang om meer ambtelijke expertise op te bouwen. Raad voor het Openbaar Bestuur, *Gezag Herwinnen. Over de gezagswaardigheid van het openbaar bestuur*, november 2022,

81. *Omzien naar elkaar, vooruitkijken naar de toekomst, Coalitieakkoord 2021-2025 VVD, D66, CDA en ChristenUnie.*

82. Kamerstukken II 2021/22, 26643, nr.

842 (herdruk).

83. *Kamerstukken II 2022/23, 26643, nr. 940.*

84. [tweedekamer.nl/sites/default/files/atoms/files/20210609\\_reikwijdte\\_takstelling\\_van\\_de\\_commissie\\_voor\\_digitale\\_zaken.pdf](https://tweedekamer.nl/sites/default/files/atoms/files/20210609_reikwijdte_takstelling_van_de_commissie_voor_digitale_zaken.pdf).

85. [tweedekamer.nl/kamerleden-en-commissies/commissies/digitale-zaken/kennisa-genda](https://tweedekamer.nl/kamerleden-en-commissies/commissies/digitale-zaken/kennisa-genda).

86. Zie bijvoorbeeld: [storage.googleapis.com/pieter-omtzigt-website/documenten/Pegasus-memorandum-Omtzigt.pdf](https://storage.googleapis.com/pieter-omtzigt-website/documenten/Pegasus-memorandum-Omtzigt.pdf).

87. *Kamerstukken II 2022/23, 36200-VII, nr. 118.*

88. In het Coalitieakkoord is in ieder geval op het gebied van de topambtenaren zelf verandering aangekondigd: ‘Bij benoemingen van topambtenaren via de Algemene Bestuursdienst wordt domeinspecifieke expertise nadrukkelijker van belang, waarbij ook de roulatiesnelheid wordt verlaagd.’ *Omzien naar elkaar, vooruitkijken naar de toekomst, Coalitieakkoord 2021-2025 VVD, D66, CDA en ChristenUnie.*