Mr. HANS VAN MIERLO STICHTING

Kanttekeningen bij de digitale stad

Gelijkheid, democratische controle en digitale autonomie in Nederlandse gemeenten

Laura de Vries

Over de Mr. Hans van Mierlo Stichting

De Mr. Hans van Mierlo Stichting (VMS) is het onafhankelijk wetenschappelijk bureau van D66. De VMS heeft tot doel het sociaal-liberale gedachtegoed verder te ontwikkelen en te verspreiden binnen en buiten D66. Dit doet zij onder andere door het uitvoeren van toegepast onderzoek naar maatschappelijke vraagstukken, het organiseren van lezingen en symposia, het geven van trainingen en workshops en het publiceren van het tijdschrift Idee en de podcast Appèl.

Omslagfoto: KanawatTH| iStock

Auteur: Laura de Vries

Vormgeving: Femke Verhelst

Mr. Hans van Mierlo Stichting
Lange Houtstraat 11
2511 CV Den Haag
www.vanmierlostichting.nl

Twitter: @VMStichting
Instagram: mr.hansvanmierlostichting
Linkedin: Mr. Hans van Mierlo Stichting
Aanmelden nieuwsbrief: vanmierlostichting@d66.nl

Inhoudsopgave

Inleiding

Gemeenten worstelen met grote uitdagingen zoals klimaatverandering, sociale en economische ongelijkheid en criminaliteit. Deze worstelingen zijn alleen maar toegenomen sinds de decentralisatie van 2015, waarbij steeds meer verantwoordelijkheden bij gemeenten zijn belegd. Nieuwe technologische toepassingen in de publieke ruimte kunnen bijdragen aan oplossingen voor deze grote uitdagingen. Hier maken gemeenten – begrijpelijkerwijs – graag gebruik van. In zogeheten smart city-projecten (hierna: slimme stad) wordt met sensoren en camera's in de publieke ruimte verkeersgedrag geanalyseerd, luchtkwaliteit gemeten, agressief gedrag herkend, duurzamer met straatlicht omgegaan, biodiversiteit beschermd en nog veel meer.

Tegelijkertijd brengen deze nieuwe technologische toepassingen ook risico's met zich mee. Niet altijd zijn de rechten van inwoners voldoende gewaarborgd. Democratische controle op deze toepassingen functioneert niet altijd goed. En gemeenten blijken vaak geen visie te hebben op hoe hun eigen autonomie beschermd moet worden tegenover commerciële partijen.
Na een eerdere publicatie van de Mr. Hans van Mierlo Stichting over het gebruik van algoritmes door lokale overheden, staan in dit onderzoek de risico's van slimme stad-projecten voor inwoners centraal. Dit paper verkent deze risico's vanuit sociaal-liberaal perspectief en doet aanbevelingen waarmee lokale politici en bestuurders technologische toepassingen in de openbare ruimte democratisch kunnen controleren.

Gelijkheid, democratische controle en digitale autonomie
§1 van dit paper beschrijft hoe technologie bij slimme stad-projecten wordt ingezet in de publieke ruimte om problemen op het vlak van bijvoorbeeld veiligheid, mobiliteit en duurzaamheid het hoofd te bieden.

In §2 staat het *gelijkheidsbeginsel* centraal. Beargumenteerd zal worden hoe slimme stad-projecten ten koste kunnen gaan van de rechten en vrijheden van inwoners. Denk aan privacy-schendingen, discriminatie, maar ook het beperken van individuele zelfbeschikking en autonomie. Met wifi-tracking kunnen inwoners via hun telefoons in de openbare ruimte gevolgd worden. Camera's en sensoren kunnen discriminatie in de hand werken wanneer zij gezichten en bewegingen van mensen van kleur niet goed herkennen. 'Slimme' lantaarnpalen beïnvloeden het gedrag van mensen door geuren te verspreiden of de kleur van het licht te veranderen. Om deze redenen is het van belang dat politieke besluiten over slimme stad-toepassingen niet alleen gebaseerd zijn op de vraag wat technologisch mogelijk is, maar dat ook de afweging wordt gemaakt wat politiek en ethisch gezien wenselijk is.

In §3 wordt besproken waarom het gebrek aan *democratische controle* op slimme stad-projecten een potentieel gevaar vormt. Veel slimme stad-projecten zijn samenwerkingen tussen een gemeente met bedrijven en/of andere overheden. Hierdoor is het lastig voor inwoners, onderzoekers en raadsleden om inzicht te krijgen in wat de projecten precies behelzen. Dit wordt versterkte door de gedachte dat slimme steden een technologische oplossing bieden voor problemen die in feite sociaal-maatschappelijk van aard zijn. Het geloof dat technologie per definitie objectief of efficiënt is, gaat

ten koste van de democratische controle op slimme steden. Zowel colleges als gemeenteraden hebben een verantwoordelijkheid om de democratische controle op slimme stad-projecten te verstevigen. De *digitale autonomie* van gemeenten staat centraal in §4. Hierin komt de vraag aan de orde wie zeggenschap heeft over wat er gebeurt met data van inwoners in slimme steden. Gemeenten met slimme stad-projecten lopen het risico afhankelijk te worden van een beperkt aantal (software) aanbieders. Hierdoor kunnen zij de zeggenschap verliezen over de manier waarop data van inwoners worden verwerkt. Wanneer het gemeentebestuur de grip verliest op dataverwerkingen, groeit het risico op het schenden van de rechten en vrijheden van inwoners en op gebrekkige democratische controle. Maatregelen voor meer digitale autonomie moeten echter niet gericht zijn op het verstevigen van de grip van gemeenten alleen, maar vooral op het beschermen en vergroten van rechten en vrijheden van inwoners.

Sociaal-liberale handvatten

Aan dit paper is een 'APK voor digitale autonomie in de slimme stad' toegevoegd. Met deze jaarlijkse keuring kunnen gemeentebesturen, raadsleden en andere belangstellenden op hoofdlijnen nagaan in hoeverre slimme stad-projecten in hun gemeente voldoen aan enkele belangrijke voorwaarden ter waarborging van hun digitale autonomie. Het ligt in de lijn der verwachting dat technologische toepassingen in de publieke ruimte de komende jaren een sterke groei zullen doormaken. Dat maakt het des te urgenter voor colleges en gemeenteraden om hun positie te bepalen tegenover dit vraagstuk. Met dit onderzoek wil de Mr. Hans van Mierlo Stichting daar sociaal-liberale handvatten voor bieden. Want pas als gemeenten op democratische wijze grip hebben op de manier waarop de data van hun inwoners worden verzameld en verwerkt, kunnen de rechten van inwoners gewaarborgd worden en hun vrijheden en mogelijkheden worden vergroot.

De ‘slimme’ stad

§1

Gemeenten kennen verschillende toepassingen van digitale technologieën. Het kan gaan om algoritmes – digitale beslisformules – die worden gebruikt om bijvoorbeeld de kans te berekenen dat iemand fraude pleegt of voortijdig school zal verlaten.[1] Andere toepassingen zijn specifiek gericht op het verzamelen en analyseren van informatie afkomstig uit de publieke ruimte. Vaak gebeurt dit binnen zogeheten ‘slimme stad’-projecten.

Slimme stad – van oorsprong een marketingterm van technologiebedrijven – is in feite een benaming voor toepassingen van informatie- en communicatietechnologie (ICT) in de openbare ruimte.[2] Dit kan in de stad zijn, maar ook daarbuiten. Toepassingen zijn vaak gericht op problemen waar vooral (grote) steden mee kampen, zoals verkeersdrukte, vervuiling en criminaliteit.[3] Bij slimme stad-projecten worden meters en sensoren in de openbare ruimte geïnstalleerd in bijvoorbeeld lantaarnpalen, afvalbakken en verkeerslichten. Denk ook aan cameratoezicht voor criminaliteitspreventie en in uitgaansgebieden om bijvoorbeeld agressie tegen te gaan. Steden hopen met deze digitale toepassingen veiliger, duurzamer en mobieler te worden.[4] Door technologieën als camera’s, sensoren en dashboards met elkaar te verbinden, ook wel *Internet of Things* (IoT) genoemd, moeten de toepassingen nog effectiever worden.

De term slimme stad dient in de praktijk als een verzamelnaam voor uiteenlopende, vaak los van elkaar functionerende projecten. Het netwerk van de veertig grote steden, het G40-Stedennetwerk, heeft een inventarisatie gedaan van slimme stad projecten in Nederland.[5] Zo heeft de gemeente Alkmaar de ‘snuffelfiets’, een fiets met sensoren die de luchtkwaliteit meten, en een Urban Mobility Lab om verkeersproblemen te analyseren. De gemeente Almelo gebruikt een app waarin inwoners meldingen kunnen doen over de openbare ruimte, heeft ‘slimme’ stoplichten en wil mogelijk verkeer gaan meten met behulp van wifi-tracking: het volgen van mensen via wifisignalen van hun telefoon. De gemeente Lelystad gebruikt drones voor landmetingen, en de gemeente Roosendaal heeft een *living lab* waar “partijen kunnen experimenteren met IoT projecten (sensoren)”.[6] Ook het aantal projecten per gemeente verschilt enorm. Waar sommige steden slechts twee projecten hebben (Haarlemmermeer, Heerlen), lopen in andere gemeenten 31 projecten (Leeuwarden) of 38 (Dordrecht).[7] Box 1, 2 en 3 lichten enkele projecten toe. Zo heeft Eindhoven een project genaamd Twin City Eindhoven (box 1). In Scheveningen werkt de gemeente Den Haag aan een living lab (box 2). En binnen veel gemeenten wordt volop geëxperimenteerd met gezichtsherkenningssoftware, zoals op Schiphol en bij verschillende voetbalclubs (box 3).

1. L. de Vries, *Algoritmes en Lokale Overheden. Kansen voor Iedereen?* (Den Haag: Mr. Hans van Mierlo Stichting, 2020), p. 27-28.
2. N. Odendaal, Information and Communication Technology and Local Governance: Understanding the Difference between Cities in Developed and Emerging Economies, *Computers, Environment and Urban Systems*, 27, nr. 6 (2003): 585-607, p. 586.
3. A. Meijer en M. Bolívar, Governing the Smart City: A Review of the Literature on Smart Urban Governance. *International Review of Administrative Sciences*, 82, nr. 2 (2016): 392-408, p. 393.
4. E. Ismagilova et al., Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework, *Information Systems Frontiers* (2020): p. 5.
5. H. Teuben et al., Smart Cities in de G40: *Overzicht Versnellers en Knelpunten en Advies* (Stedennetwerk G40, 2020).
6. Teuben et al., *Smart Cities in de G40*, p. 119.
7. Ibidem, p. 55.

Box 1. Tweelingstad Eindhoven

De gemeente Eindhoven heeft een project genaamd Twin City Eindhoven. De gemeente wil een zogenoemde 'digitale kopie' maken van de stad. In een dashboard zien ambtenaren een digitale weergave van de stad, met informatie over bebouwing, natuur en type huishoudens.[8] Data die opgevangen worden uit camera's en sensoren moeten real time worden doorgegeven. Meer dan 125 datasets zouden in de *digital twin* in Eindhoven worden gecombineerd.[9] Ambtenaren krijgen zo inzicht in ontwikkelingen in de stad, zoals de doorstroom van mensen en voertuigen, luchtvervuiling of de aanwezigheid van groen.[10] Ook zouden zij plannen voor de publieke ruimte, bijvoorbeeld het verbreden van een weg of het aanleggen van groen, eerst kunnen testen in de digitale versie van de stad.[11] De impact van beleidsinterventies kan zo met een digital twin worden doorberekend.[12] Onderscheidend aan het concept van een digital twin is dat fysieke objecten, zoals camera's of sensoren, via het dashboard aangestuurd zouden kunnen worden, ook zonder dat hier een mens aan te pas komt.[13] Naast de gemeente Eindhoven zijn ook de gemeenten Helmond en Almere bezig met een digital twin-project.[14]

Box 2. Levend laboratorium in Scheveningen

De gemeente Den Haag werkt aan een levend laboratorium (een zogeheten living lab) in Scheveningen. Sensoren en camera's worden gemonteerd aan straatmeubilair en verbonden via een glasvezelnetwerk. Het doel is onder andere om afval en geluidsoverlast tegen te gaan en via natuurtellingen de biodiversiteit in de gaten te houden.[15] De sensoren registreren onder meer de geluidssterkte van muziek, verkeer en stemmen.[16] De gemeente wil met behulp van kunstmatige intelligentie geluidsvoorspellingen doen, gebaseerd op geluiden uit het verleden en geluidsmeldingen van omwonenden.[17] Met camera's worden druktemetingen gedaan, en kunstmatige intelligentie wordt ook ingezet om dieren te tellen, om zo zicht te krijgen op onder andere de vleermuizenpopulatie. Bezoekers aan de Scheveningse boulevard worden via digitale informatieschermen en kunstprojecten geïnformeerd over de dataverwerkingen.

8. 3D Digital Twin – Eindhoven, Argaleo, geraadpleegd op 3 maart 2022 van https://www.youtube.com/watch?v=9v-_iUd9Kp8.
9. Ibidem.
10. T. Deng, K. Zhang, en Z.-J. Shen, A Systematic Review of a Digital Twin City: A New Pattern of Urban Governance Toward Smart Cities, *Journal of Management Science and Engineering*, 6, nr. 2 (2021): 125-134, p. 128.
11. Digital twinning is SimCity met echte steden, *Cursor*, 23 maart 2021, geraadpleegd van https://www.cursor.tue.nl/nieuws/2021/maart/week-4/digital-twinning-is-simcity-met-echte-steden/.
12. Autoriteit Persoonsgegevens, Smart Cities: *Onderzoeksrapport bescherming van persoonsgegevens in de ontwikkeling van Nederlandse Smart Cities* (2021), p. 28.
13. L. Deren, Y. Wenbo, en S. Zhenfeng, Smart City based on Digital Twins, *Computational Urban Science*, 1, nr. 4 (2021): p. 1-2.
14. De Digital Twin van Geodan, Brainport Smart District, geraadpleegd op 8 maart 2022 van https://brainportsmartdistrict.nl/project/de-digital-twin-van-geodan/; Teuben et al., *Smart Cities in de G40*, p. 63.
15. S. Bruines, Voortgang Living Lab Scheveningen, RIS305831, *Gemeente Den Haag*, 22 juli 2020.
16. S. Bruines, Voortgang Living Lab Scheveningen, RIS309315, *Gemeente Den Haag*, 12 juli 2021.
17. T. Verheijen, Living Lab: leren door te doen: Smart City Den Haag oefent 'op Scheveningen', *Computable*, 11 oktober 2021, geraadpleegd van https://www.computable.nl/artikel/achtergrond/magazine/7256793/5215853/living-lab-leren-door-te-doen.html.

Bij slimme stad-projecten ligt techno-solutionisme op de loer.

Box 3. Gezichtsherkenningscamera's in Den Bosch en op Schiphol

In de Korte Putstraat in Den Bosch werden in 2019 carnavalsvierders geïdentificeerd via camera's door de gemeente in samenwerking met een commerciële organisatie. Het doel was mensen te herkennen die een straatverbod hadden en zich toch op straat begaven. Volgens softwareleverancier CrowdWatch was angst voor privacy-schending overbodig, omdat de software alleen zou kijken "naar mensen die al iets misdaan hebben".[18] Toch zijn om onderscheid te kunnen maken tussen gewenste en ongewenste bezoekers ruim elfduizend gezichten gescand.[19] Het gemeentebestuur in Almere wil mogelijk pilots gaan uitvoeren met 'slimme' camera's voor handhaving.[20] In Eindhoven gebruikt de gemeente camera's voor het herkennen van geweld. Met behulp van kunstmatige intelligentie en een 'algoritmeplatform' zouden incidenten in uitgaansgebieden voorkomen moeten worden. Gezichtsherkenning wordt hier volgens de gemeente niet bij gebruikt.[21] Op Schiphol wordt geëxperimenteerd met gezichtsherkenning bij een pilot met 'biometrisch boarden', waar het gezicht fungeert als identiteitsbewijs.[22] De Universiteit Leiden gebruikte in 2021 camera's voor het tellen van studenten. Volgens het universiteitsblad Mare waren de camera's ook in staat om het geslacht, de leeftijd en zelfs het humeur van mensen te registeren. Het universiteitsbestuur zegt dat de camera's niet voor deze doeleinden gebruikt werden. Ook voetbalclubs experimenteren volop met camera's. Bij FC Den Bosch hingen in 2019 camera's met gezichtsherkenning. ADO Den Haag gebruikt naar eigen zeggen ook gezichtsherkenning bij binnenkomst van het stadion.

18. B. Gotink, Slimme camera's herkennen elke carnavalsvierder in Korte Putstraat: 'Wie er niet in mag, hebben we er zo uitgepikt', *Brabants Dagblad*, 6 maart 2019, geraadpleegd van https://www.bd.nl/den-bosch-vught/slimme-camera-s-herkennen-elke-carnavalsvierder-in-korte-putstraat-wie-er-niet-in-mag-hebben-we-er-zo-uitgepikt~a55f6fdd/.
19. Ibidem.
20. Cameratoezicht aan vervanging toe; burgemeester wil slimme camera's, *Omroep Flevoland*, 12 juni 2020, geraadpleegd van https://www.omroepflevoland.nl/nieuws/182268/cameratoezicht-aan-vervanging-toe-burgemeester-wil-slimme-camera-s.
21. Teuben et al., *Smart Cities in de G40*, p. 37.
22. Proef met gezichtsherkenning bij vertrek, *Schiphol*, geraadpleegd op 8 maart 2022 van https://www.schiphol.nl/nl/pagina/proef-met-gezichtsherkenning-bij-vertrek/.

Experimenten met technologie mogen niet leiden tot experimenten met de rechten en vrijheden van inwoners.

De grote beloftes van de slimme stad

Slimme stad-experimenten doen grote beloftes. Regelmatig wordt een slimme stad hierdoor gezien als "een hemelsblauwe oase waarin alles efficiënt en foutloos verloopt", schrijft het Rathenau Instituut in het rapport Voeten in de Aarde. Dat dit lang niet altijd het geval is, bleek bijvoorbeeld in Assen. Daar wilde het gemeentebestuur in 2006 honderden sensoren plaatsen in de publieke ruimte bij het project Sensor City. Het gemeentebestuur omschreef het project als "een proeftuin en etalage tegelijk voor toepassingen van sensortechnologie". In 2018 werd het project vanwege geldproblemen stopgezet. Uit een evaluatie van de gemeente bleek het "niet realistisch" te verwachten dat binnen tien tot vijftien jaar zo'n groot netwerk van sensoren gebouwd kon worden. Bovendien had het gemeentebestuur verschillende rollen in het project, die niet goed met elkaar samengingen. Dit bestuur was namelijk zowel de verbindende partij als ambassadeur en toezichthouder op het project. Bovendien ontbrak het aan een inhoudelijke discussie over het project, doordat het onderwerp niet vaak genoeg op de politieke agenda stond.

Bij slimme stad-projecten ligt techno-solutionisme op de loer. Dit houdt in dat technologie gezien wordt als een oplossing voor sociaal-maatschappelijke problemen, terwijl maatschappelijke problemen nooit met alleen technologie opgelost kunnen worden. Econoom Mariana Mazzucato noemde slimme steden dan ook "onrealistische technologische wondermiddelen". Sommige wetenschappers beschouwen digital twins wel als "een nieuw beginpunt voor de bouw van moderne smart cities" dat verkeersdrukte zou kunnen tegengaan, en kansen biedt voor inwonerparticipatie via Virtual Reality. Judith Veenkamp van onderzoeksinstituut Waag waarschuwt echter dat een digital twin niet gezien moet worden als een "heilige graal" om structurele problemen op te lossen. Slimme stad-toepassingen kunnen slechts fungeren als onderdeel van een breder pakket aan maatregelen om structurele problemen – zoals luchtvervuiling, geluidsoverlast of onveiligheid – aan te pakken.

23. A. Kloosterman en M. Reid, Opeens hangen er overal slimme camera's (en die zien alles), *Mare*, 17 november 2021, geraadpleegd van https://www.mareonline.nl/achtergrond/opeens-hangen-er-overal-slimme-cameras-en-die- zien-alles/.
24. Voorwaarden, *ADO Den Haag*, geraadpleegd op 8 maart 2022 van https://adodenhaag.nl/nl/tickets/voorwaarden.
25. B. Karstens et al., *Voeten in de Aarde: Datagestuurde innovatie in de stad* (Den Haag: Rathenau Instituut, 2020), p. 13.
26. Notitie: Ontwikkeling van het sensor cluster, raadsvergadering 4 juli 2013, *Gemeente Assen*, geraadpleegd van https://assen.bestuurlijkeinformatie.nl/Agenda/Index/b24f3563-6a3d-49c7-a67f-7be387c3da2f.
27. Brief B&W, Evaluatie Sensor Cluster Gemeente Assen, *Gemeente Assen*, 29 december 2016, geraadpleegd van https://assen.bestuurlijkeinformatie.nl/Agenda/Index/304ddf0a-70ef-438a-9c0f-e3730b5a71c0.
28. Karstens et al., *Voeten in de aarde*, p. 13.
29. M. Mazzucato, *Mission Economy: A Moonshot Guide to Changing Capitalism* (London: Allen Lane, 2021), p. xxi.
30. L. Dieren, Y. Wenbo, en S. Zhenfeng, Smart City based on Digital Twins, *Computational Urban Science*, 1, nr. 4 (2021): p. 10.
31. F. Dembski, U. Wössner, en M. Letzgus, The Digital Twin Tackling Urban Challenges with Models, Spatial Analysis and Numerical Simulations in Immersive Virtual Environments, *Data – Smart Cities*, 1 (2019): 795-804, p. 802.
32. Autoriteit Persoonsgegevens, *Smart Cities*, p. 28.
33. Karstens et al., *Voeten in de Aarde*, p. 13.

Gelijkheidsbeginsel

§2

Volgens het gelijkheidsbeginsel (artikel 1 van de Grondwet) zou iedereen in gelijke gevallen gelijke rechten moeten hebben en een gelijke behandeling moeten krijgen. Bij bepaalde slimme stad-toepassingen dreigt dit principe in gevaar te komen. Deze paragraaf gaat in op de oorzaken hiervan, en stipt enkele ontwikkelingen aan die het risico hierop vergroten.

Een van de oorzaken van discriminatie door technologie, is dat technologie nog altijd vaak wordt gezien als objectief en neutraal. In tegenstelling tot mensen hebben computers geen last van vooroordelen, is vaak de gedachte. Technologie wordt echter door mensen gebouwd. In het verzamelen en het verwerken van data zitten allerlei keuzes verstopt, bijvoorbeeld voor de selectie en herkomst van de data, de manier waarop data worden geanalyseerd en de uitkomsten worden gebruikt. Als deze keuzes gebaseerd zijn op vooroordelen, kunnen technologische toepassingen net zo goed discriminatie in de hand werken. Sterker nog, met bevooroordeelde technologie kan discriminatie worden geautomatiseerd, wat op enorme schaal gevolgen kan hebben voor mensen.[34] Experimenten met technologie – hoe belangrijk ook – mogen niet leiden tot experimenten met de rechten, kansen en vrijheden van inwoners.

Biometrie

Biometrie betekent het meten van fysieke of gedragskenmerken van mensen. Voorbeelden hiervan zijn bewegingssensoren, gezichtsscans, stem- of emotieherkenning. Biometrie is vaak onderdeel van slimme stad-projecten, vooral stem- en bewegingssensoren. Denk aan lantaarnpalen met sensoren en camera's waarmee mogelijk agressief stemgeluid of gedrag kan worden gesignaleerd.[35]

Het toepassen van biometrie kan discriminatie en uitsluiting in de hand werken en versterken.[36] Biometrische software herkent bijvoorbeeld niet altijd de bewegingen en gezichten van zwarte mensen en met name zwarte vrouwen, doordat deze software vaak voornamelijk wordt 'getraind' met beeldmateriaal van witte mensen, en voornamelijk witte mannen.[37] Denk aan sensoren in draaideuren van gebouwen die de bewegingen van zwarte mensen als zodanig niet herkennen. Ook de sensoren in zelfrijdende auto's zouden witte mensen beter herkennen dan zwarte mensen, met als gevolg dat zwarte mensen door deze auto's eerder aangereden kunnen worden dan witte mensen.[38] Ook gezichtsherkenningssoftware waarmee mensen kunnen worden ingedeeld in de categorieën vrouw/man kan de al bestaande uitsluiting van non-binaire personen automatiseren.[39]

Het besef dat biometrische software inclusiever ontworpen moet worden, is de afgelopen jaren flink gegroeid. Technologiebedrijven realiseren zich dat mensen van kleur vertegenwoordigd moeten zijn in de trainingsdata, willen ze software ontwikkelen die niet leidt tot discriminatie. Maar dit gebeurt niet altijd op een eerlijke en rechtvaardige manier. Google experimenteerde bijvoorbeeld in 2019 in Atlanta en Los Angeles met

34. C. O'Neill, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, (New York: Crown Publishers, 2016), p. 29-30.
35. D. Snijders et al., *Burgers en Sensoren: Acht Spelregels voor de Inzet van Sensoren voor Veiligheid en Leefbaarheid* (Den Haag: Rathenau Instituut, 2020), p. 39 en 74.
36. R. Benjamin, *Race after technology. Abolitionist Tools for the New Jim Code* (Cambridge: Polity Press, 2019), p. 17.
37. J. Buolamwini en T. Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, *Proceedings of Machine Learning Research*, 81 (2018): p. 77-91.
38. B. Wilson, J. Hoffman, en J. H. Morgenstern, Predictive Inequity in Object Detection, *Computer Science* (2019): p. 9.
39. D. Leufer, Computers are Binary, People are Not: How AI Systems Undermine LGBTQ Identity, *Access Now*, 6 april 2021, geraadpleegd van https://www.accessnow.org/how-ai-systems-undermine-lgbtq-identity/.

gezichtsherkenningssoftware op de gezichten van dakloze mensen van kleur.[40] De Chinese overheid traint haar gezichtsherkenningssoftware door deze te verkopen aan landen in Afrika, bijvoorbeeld Zimbabwe, om zo gezichten van mensen van kleur te kunnen analyseren.[41] Sociale en economische uitbuiting is bovendien staande praktijk bij sommige grote technologiebedrijven. Zo worden contentmoderatoren – mensen die de berichten op het sociale mediaplatform modereren – van Facebook (nu 'Meta') structureel blootgesteld aan traumatiserende inhoud. Een initiatief van werknemers in Kenia om een vakbond op te richten en zo te pleiten voor betere werkomstandigheden, werd door het bedrijf in de kiem gesmoord.[42]

Als biometrie wordt gebruikt in de openbare ruimte, bijvoorbeeld door de politie om verdachten op te sporen, kan dit grote gevolgen hebben. Mensen met eigenschappen waarop het systeem minder betrouwbaar reageert, kunnen hierdoor bijvoorbeeld vaker onterecht staande worden gehouden. Biometrische identificatie wordt bovendien vaak gebruikt om gemarginaliseerde groepen te surveilleren en uit te sluiten, zoals migranten of mensen die dak- of thuisloos zijn.[43] Slimme stad-toepassingen kunnen op deze manier een versterkend effect hebben op bestaande sociale ongelijkheid.[44] Bovendien hebben inwoners in feite geen uitweg in een slimme stad: het is immers hun leefomgeving. Dat maakt het vrijwel onmogelijk om aan de dataverwerking te ontkomen.[45] AI in 2015 waarschuwde het Rathenau Instituut dat bezwaar maken tegen dataverwerkingen door overheden lastig is.[46] Dit geldt zeker voor mensen met weinig digitale vaardigheden, wat de digitale kloof dreigt te vergroten.[47] Gezichtsherkenningssoftware kan ook worden gebruikt om de kans te berekenen wat iemands seksualiteit of zelfs politieke voorkeur is.[48] Biometrie die voor deze doeleinden wordt gebruikt, vormt een inbreuk op zowel de privacy als de autonomie van individuen. Een belangrijk onderdeel van autonomie is namelijk de mogelijkheid om een persoonlijke identiteit te vormen aan de hand van eigen keuzes.[49] Het herkennen van mensen door een gezichtsherkenningssysteem miskent de uniekheid van het individu en hindert de vorming van een persoonlijke identiteit.[50] Wanneer gezichtsherkenning het handelen van de overheid richtig burger (mede) bepaalt, beperkt dit de autonomie en zelfbeschikking van individuen.

Niet voor niets is het gebruik van biometrische gegevens in de publieke ruimte zeer omstreden. In het Verenigd Koninkrijk hebben burgerrechtenactivisten een rechtszaak aangespannen wegens het gebruik van gezichtsherkenningssoftware door de politie in Zuid-Wales. Tussen 2017 en 2018 heeft de politie daar ongeveer 500.000 gezichten gescand. De rechter oordeelde dat het gebruiken van gezichtsherkenningssoftware de privacy schond en onvoldoende was onderzocht of met het systeem niet gediscrimineerd werd.[51]

Ook de Europese Commissie heeft zich uitgesproken over biometrie in de publieke ruimte. Zo wordt in de AI-Verordening van de Europese Commissie het gebruik van gezichtsherkenning verboden, tenzij er een geldende reden is om het wel te gebruiken, bijvoorbeeld bij terroristische dreiging of voor de beveiliging

40. S. Fussell, How an Attempt at Correcting Bias in Tech Goes Wrong, *The Atlantic*, 9 oktober 2019, geraadpleegd van https://www.theatlantic.com/technology/archive/2019/10/google-allegedly-used-homeless-train-pixel-phone/599668/.
41. A. Hawkins, Beijing's Big Brother Tech Needs African Faces: Zimbabwe is Signing up for China's Surveillance State, but its Citizens will Pay the Price, *Foreign Policy*, 24 juli 2018, geraadpleegd van https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/.
42. B. Perrigo, Inside Facebook's Sweatshop, *Time*, 14 februari 2022, laatst aangepast op 17 februari 2022 geraadpleegd van https://time.com/6147458/facebook-africa-content-moderation-employee-treatment/.
43. Professor Ruha Benjamin – Obert C. Tanner Lecture on AI and Human Values 2021, *Clare Hall, University of Cambridge*, 13 december 2021, minuut 16:03-17:48, geraadpleegd van https://www.youtube.com/watch?v=e3MQum7HrVM&t=1991s.
44. A. Voorwinden, The Privatised City: Technology and Public-Private Partnerships in the Smart City, *Law, Innovation and Technology*, 13, nr. 2 (2021): 439-463, p. 455.
45. Ibidem.
46. L. Kool, J. Timmer, en R. van Est, *De Datagedreven Samenleving* (Den Haag: Rathenau Instituut, 2015), p. 12.
47. A. Vennekens, Digitale Vaardigheden voor Technologisch Burgerschap, *Rathenau Instituut*, 10 februari 2022, geraadpleegd van https://www.rathenau.nl/nl/wetenschap-cijfers/impact/kennis-voor-maatschappelijke-uitdagingen/digitale-vaardigheden-voor?utm_medium=email.
48. M. Kosinski, Facial Recognition Technology Can Expose Political Orientation from Naturalistic Facial Images, *Scientific Reports*, 11, nr. 200 (2021): p. 2-4.
49. A. Vugts et al., How Autonomy is Understood in the Ethics of Nudging, *Behavioural Public Policy*, 4, nr. 1 (2020): 108-123, p. 118.
50. R.A. Waelen, The struggle for recognition in the age of facial recognition technology, *AI and Ethics* (2022): p. 4.
51. R (Bridges) V The Chief Constable of South Wales Police & others, EWCA Civ 1058, *Royal Courts of Justice*, 11 augustus 2020, geraadpleegd van https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf.

van een kerncentrale.[52] Ook hebben de Autoriteit Persoonsgegevens en de Europese toezichthouder voor bescherming van persoonsgegevens gepleit voor een algeheel verbod op gezichtsherkenning.[53] Des te opvallender is dat in Nederland nog steeds op openbare plekken gezichtsherkenningssoftware wordt gebruikt (§1, box 3), en dat ook de Nationale Politie van dergelijke software gebruikmaakt.

Gedragssturing door technologie

Een ander risico van slimme stad-toepassingen is onwenselijke gedragsbeïnvloeding. Technologische toepassingen in de openbare ruimte bieden niet alleen de mogelijkheid om gedrag van mensen te analyseren, maar ook om gedrag te sturen. Zo moesten de slimme lantaarnpalen bij het Stratumseind in Eindhoven agressie tegengaan door van lichtkleur te veranderen. Het onbewust beïnvloeden van mensen zodat zij 'wenselijk' gedrag gaan vertonen, wordt ook wel nudging genoemd. Nudging kan echter ook overgaan in manipulatie. Van manipulatie is sprake wanneer iemands beslissingscapaciteit wordt beïnvloed zonder dat diegene zich hiervan bewust is. Manipulatie leidt ertoe dat mensen een keuze maken die zij anders niet hadden gemaakt, of dat zij handelen op basis van redenen die buiten henzelf liggen.[54] Sociale mediaplatforms zijn hiervan het meest duidelijke voorbeeld: aan de hand van persoonlijke profielen worden mensen gemanipuleerd tot het vormen van een politieke voorkeur of het doen van bepaalde aankopen.[55] Ook in de openbare ruimte kunnen profielen van mensen worden gebruikt voor advertenties. In 2017 kregen mensen bijvoorbeeld op reclameborden op station Amersfoort en Amsterdam Centraal advertenties te zien afhankelijk van hun uiterlijke kenmerken. Camera's in billboards registreerden geslacht of leeftijd, en afhankelijk daarvan werden specifieke reclames getoond.[56] De Autoriteit Persoonsgegevens publiceerde naar aanleiding hiervan een toelichting op het gebruik van camera's in reclamezuilen.[57] Daarnaast maken gemeenten volop gebruik van wifi- of bluetooth-tracking. Via de wifi- of bluetooth-signalen van telefoons wordt zo bijvoorbeeld het aantal bezoekers in winkelstraten geteld, en kunnen zij zelfs gevolgd worden. De gemeente Enschede kreeg in maart 2021 een boete van 600.00 euro van de Autoriteit Persoonsgegevens voor het gebruiken van wifi-tracking. Volgens de toezichthouder was het met de wifi-tracking mogelijk om "winkelend publiek en mensen die in de binnenstad wonen of werken te volgen."[58] Wifi- en bluetoothtracking kunnen ook worden gebruikt voor het bieden van gerichte advertenties op telefoons. De voormalig minister van rechtsbescherming Sander Dekker gaf in april 2019 aan dat niet bekend was in welke gemeenten wifitracking wordt toegepast.[59]

Technologie in de openbare ruimte kan dus manipulatief worden wanneer deze mensen stuurt in hun besluitvorming zonder dat zij zich hier bewust van zijn. Nudging en manipulatie hebben invloed op de individuele autonomie, oftewel de mogelijkheid om het leven naar eigen inzicht vorm te geven. Het maken van betekenisvolle, onafhankelijke keuzes is hier een fundamenteel onderdeel van.[60] Volgens onderzoekers van de Universiteit Utrecht kan de optelsom van *nudges* zelfs zo ver gaan dat het leidt tot een

52. COM(2021) 206 final.
53. A. Jelinek, en W.R. Wiewiórowski, *Joint Opinion on the proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence* (Artificial Intelligence Act), EDPB-EDPS (Brussel, 2021), p. 2-3.
54. D. Susser, B. Rössler, en H. Nissenbaum, Technology, Autonomy, and Manipulation, *Internet Policy Review*, 8, nr. 2 (2019), p. 8.
55. D. Susser, B. Rössler, en H. Nissenbaum, Technology, Autonomy, and Manipulation, *Internet Policy Review*, 8, nr. 2 (2019), p. 8-13.
56. J. Schellevis, Reclameborden op A'dam CS weten wanneer en hoelang jij kijkt, *NOS*, 4 september 2017, geraadpleegd van https://nos.nl/artikel/2191341-reclameborden-op-a-dam-cs-weten-wanneer-en-hoelang-jij-kijkt.
57. A. Wolfsen, Normenkader digitale billboards, *Autoriteit Persoonsgegevens*, 25 juni 2018, geraadpleegd van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_branche_normkader_digitale_billboards.pdf.
58. Boete gemeente Enschede om wifitracking, *Autoriteit Persoonsgegevens*, 11 maart 2021, geraadpleegd van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_ap_gemeente_enschede.pdf.
59. Aanhangsel Handelingen II 2019/20, S. Dekker. Antwoorden Kamervragen over wifitracking.
60. Susser, Rössler, en Nissenbaum. Technology, Autonomy, and Manipulation, p. 8.

'identiteitsparadox', waarbij het niet mensen zelf, maar algoritmes zijn die de identiteit van individuen vormgeven en zijn of haar keuzes bepalen.[61] Individuen vormen namelijk hun identiteit aan de hand van "keuzes die zij maken, doelen die zij nastreven en de waarden die zij met zich dragen"[62]; iets dat door te veel nudging in gevaar komt. Ook het 'niet-handelen' kan een consequentie zijn van onwenselijk technologiegebruik. Wanneer mensen geen gebruik maken van een bepaald recht of vrijheid als gevolg van technologiegebruik, treedt het *chilling effect* op.[63] Van een *chilling effect* is bijvoorbeeld sprake wanneer iemand niet gaat demonstreren uit angst om via cameratoezicht herkend te worden door autoriteiten. Uit een vragenlijst van de politie in Londen bleek bijvoorbeeld dat 38 procent van de ondervraagden tussen de 16 en 24 jaar weg zou blijven van evenementen of bijeenkomsten wanneer er gezichtsherkenningssoftware zou worden gebruikt.[64] Volgens onderzoekers van de Universiteit Utrecht zou de aanwezigheid van een *chilling effect* kunnen wijzen op een schending van het grondrecht op individuele autonomie.[65]

61. M.J. Vetzo, J.H. Gerards, en R. Nehmelman, *Algoritmes en Grondrechten* (Den Haag: 2018), p. 129.
62. Vugts et al., How Autonomy is Understood in the Ethics of Nudging, p. 118.
63. Vetzo, Gerards, en Nehmelman, *Algoritmes en Grondrechten*, p. 127-130.
64. S. Shale et al., *Final Report on Live Facial Recognition* (London Policing Ethics Panel, 2019), p. 7.
65. Vetzo, Gerards, en Nehmelman, s, p. 128-130.

Democratische controle

§3

Een tweede principe dat onder druk kan komen te staan door slimme stad-projecten is democratische controle. Democratische controle van slimme steden ligt grotendeels bij de gemeenteraden, die de uitvoering van beleid door het college van burgemeester en wethouders controleren. Er is een aantal factoren dat het gebrek aan democratische controle op slimme stad-projecten bemoeilijkt.

Bij het ontwikkelen van software voor slimme stad-toepassingen worden belangrijke keuzes gemaakt die de levens van inwoners direct kunnen raken. §2 liet bijvoorbeeld zien dat het gebruiken van gezichtsherkenningssoftware kan leiden tot discriminatie wanneer de software vooral is getraind op beeldmateriaal van witte mensen. Volgens Reijer Passchier, universitair docent aan de Universiteit Leiden en de Open Universiteit, verschuift door digitalisering de zogeheten discretionaire bevoegdheid – de ruimte die ambtenaren hebben om binnen het wettelijk kader naar eigen inzicht te handelen – langzaam van ambtenaren naar softwareprogrammeurs.[66] Programmeurs oefenen via de door hen geprogrammeerde computersystemen hierbij een 'dwingende macht' uit op inwoners, aldus Passchier.[67] Hij laat zien dat bedrijven echter niet dezelfde democratische legitimiteit hebben als overheden in het maken van dergelijke keuzes. Dit raakt dan ook het functioneren van de democratie en rechtsstaat.[68]

De Raad van State schreef in een ongevraagd advies in 2018 dat bij digitalisering van besluitvorming de burger niet meer na kan gaan "welke regels zijn toegepast en het niet meer [is] vast te stellen of de regels ook werkelijk doen waarvoor ze bedoeld zijn."[69] Dit wordt versterkt doordat bedrijven weinig inzicht bieden in de werking van hun software en data-analyses.[70] Vaak geven zij als reden hiervoor dat het gaat om bedrijfsgeheimen, en dat het delen hiervan hun concurrentiepositie ten opzichte van andere bedrijven kan verzwakken.[71]

Dit maakt het lastiger voor burgers, onderzoekers, raadsleden en zelfs voor het college van burgemeester en wethouders om inzicht te krijgen in hoe de software werkt. Dit verzwakt de democratische controle op slimme stad-projecten, terwijl de werking daarvan grote gevolgen kan hebben voor de rechten, kansen en vrijheden van inwoners. In deze context spreekt Reijer Passchier ook wel over digitaal feodalisme: "Een systeem waarin grote techbedrijven in staat zijn om burgers hun regelorde op te leggen, zonder dat die desgewenst gecorrigeerd kan worden met democratisch gelegitimeerde wetgeving."[72]

Ook aan de kant van de controleurs gaat het vaak mis. Digitalisering staat namelijk niet voldoende op de agenda bij gemeenteraden en -besturen. Uit onderzoek van het Rathenau Instituut blijkt dat politici en bestuurders digitalisering veelal zien als een uitvoeringsvraagstuk, in plaats van een thema voor op de lokale politieke agenda.[73] Het politieke debat gaat bovendien te vaak over incidenten en te weinig over de onderliggende vraagstukken, zoals de wenselijkheid van een toepassing en de onderliggende waarden die in het gedrang kunnen

66. R. Passchier, *Artificiële Intelligentie en de rechtsstaat: Over verschuivende overheidsmacht, Big Tech en de noodzaak van constitutioneel onderhoud* (Den Haag: Boom Juridisch, 2021), p. 61-67.
67. Ibidem, p. 65.
68. Ibidem, p. 65-66.
69. Kamerstukken II 2018, 50999, p. 3.
70. R. de Lange en J. Leupen, Meerderheid Nederlandse bedrijven voldoet na drie jaar nog niet aan privacywet, *Het Financieele Dagblad*, 5 april 2021, geraadpleegd van https://fd.nl/economie-politiek/1379255/meerderheid-nederlandse-bedrijven-voldoet-na-drie-jaar-nog-niet-aan-privacywet-vol1caWlLkX2.
71. In de praktijk zijn er tussen geheimhouding en openbaarmaking ook nog tussenwegen, zoals het omschrijven of uitleggen van systemen. De gemeente Amsterdam heeft principes voor verschillende soorten transparantie, namelijk technisch, procedureel en uitlegbaarheid, vastgelegd in standaardcontracten met leveranciers. Zie: https://www.amsterdam.nl/innovatie/digitalisering-technologie/algoritmen-ai/contractvoorwaarden-algoritmen/.
72. Passchier, *Artificiële Intelligentie en de rechtsstaat*, p. 23.
73. D. Das et al., *Raad weten met digitalisering: Hoe de gemeenteraad kan sturen op de maatschappelijke impact van digitale technologie* (Den Haag: Rathenau Instituut, 2020), p. 20.

Bedrijven bieden weinig inzicht in de werking van hun software en data-analyses.

zijn. Ook de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) concludeerde in november 2021 dat er te vaak sprake is van politieke reacties op incidenten die te maken hebben met digitalisering, in plaats van dat de overheid de regie neemt.[74]

Daarnaast geven gemeentebesturen niet altijd duidelijkheid over slimme stad-projecten. In de eerste plaats zijn de beschrijvingen van de projecten vaak niet helder. Zo omschrijft de gemeente Oss in het slimme stad-overzicht van het G40 stedennetwerk een van haar projecten als een "data-gedreven manier van werken waar de leefbaarheid van een woonwijk wordt vergroot met als uitgangspunt de data die hierover bekend is, in het bijzonder de kwaliteit hiervan."[75] Daarnaast worden gemeenteraadsleden niet altijd goed betrokken door het college in besluiten over slimme stad-projecten. Dit blijkt bijvoorbeeld uit stukken van de gemeenteraad in Apeldoorn. Gemeenteraadsleden spraken daar van een gebrek aan transparantie en helderheid, en onjuiste informatie van het college over het installeren van 5G in de gemeente door het Oostenrijkse bedrijf RadioLED.[76]

Een andere ontwikkeling is dat steeds meer (digitaliserings)projecten in samenwerkingsverbanden tussen gemeenten plaatsvinden, waarop minder democratische controle bestaat.[77] Raadsleden controleren namelijk de gemeenteraad, en niet de samenwerkingsverbanden. Onderzoekers spreken in deze context ook wel over een mismatch tussen het niveau waarop gecontroleerd wordt - de gemeenteraad - en het niveau waarop veel besluiten plaatsvinden - binnen regionale samenwerkingen. Hierdoor dreigen raadsleden de grip op besluitvorming te verliezen.[78] De Raad voor het Openbaar Bestuur noemt de regio ook wel een "niemandsland" vanwege het gebrek aan democratische legitimiteit.[79] Een wet in de maak - de Wet gegevensverwerking door samenwerkingsverbanden - gaat het mogelijk nog eenvoudiger maken voor lokale en regionale overheden en bedrijven om gegevens met elkaar te delen. De Eerste Kamer moet op moment van schrijven nog over het aannemen van de wet beslissen. De Autoriteit Persoonsgegevens heeft deze wet in november 2021 afgeraden.[80]

74. C. Prins et al., *Opgave AI. De Nieuwe Systeemtechnologie* (Den Haag: Wetenschappelijke Raad voor het Regeringsbeleid, 2021), p. 17.
75. Teuben et al., *Smart Cities in de G40*, p. 118.
76. Aangaan beschikbaarheidsovereenkomst RadioLED, *Gemeente Apeldoorn*, 16 juli 2020, geraadpleegd van https://apeldoorn.parlaeus.nl/user/search/action=showpt/item=58048/Verslag_RadioLed.pdf.
77. M.L. Adriaanse, Wat heeft IJsselstein nog te zeggen over IJsselstein? Macht van de kiezer wordt in gemeenten steeds kleiner, *NRC*, 18 februari 2022, geraadpleegd van https://www.nrc.nl/nieuws/2022/02/18/wat-heeft-ijsselstein-nog-te-zeggen-over-ijsselstein-macht-van-de-kiezer-wordt-in-gemeenten-steeds-kleiner-a4090588.
78. K. Peters, en P. Castenmiller (red.), *Controle als democratische waarde: verslag van een verkenning van controle en verantwoording in het lokale bestuur* (Universiteit Maastricht en Stichting Decentraalbestuur.nl, 2021), p. 136.
79. M. Mekel, Regionale politiek: wie krijgt wat, wanneer en op welke manier? *Raad voor het Openbaar Bestuur*, 30 juni 2021, geraadpleegd van https://www.raadopenbaarbestuur.nl/actueel/weblogs/weblog/2021/regionale-politiek-wie-krijgt-wat-wanneer-en-op-welke-manier.
80. Kamerstukken I 2020/21, 35447, nr. G.

Box 4. Openheid over algoritmes

Naar aanleiding van de publicatie *Algoritmes en lokale overheden: kansen voor iedereen?* hebben gemeenteraadsleden in zestien gemeenten vragen gesteld aan het college over het gebruik van algoritmes.[81] Uit de antwoorden bleek dat enkele gemeentes pilots met algoritmes hebben of hebben stopgezet. Zo had het gemeentebestuur van Leidschendam-Voorburg een project waarbij met behulp van machine learning fraude met bijstandsuitkeringen opgespoord werd. Het algoritmische systeem bleek "minder objectief" dan het college had verwacht, en is daarom door het college stopgezet.[82] Ook gemeenteraadsleden in Goes hebben raadsvragen gesteld over het gebruik van algoritmes. Daar wees het college de raadsleden op een regionaal samenwerkingsverband waarbij algoritmes worden gebruikt. Het college kon hierover geen verdere toelichting geven aan de gemeenteraad, want de datasets "zijn niet beschikbaar voor de gemeente Goes".[83] Dit is opvallend, omdat het gemeentebestuur aangaf dat juist deze algoritmes de meeste ethische risico's met zich meebrengen. Het project blijft op deze manier buiten het zicht van de gemeenteraad, wat de democratische controle hierop bemoeilijkt.

Function creep

Ook zogeheten function creep vormt een risico voor de democratische controle op slimme stad-toepassingen. Hiervan is sprake wanneer (op democratische wijze) is besloten dat technologie voor een bepaald doel kan worden gebruikt, maar deze in de praktijk ook gebruikt wordt voor ander doeleinden. Dit blijkt in de praktijk verleidelijk. De Nederlandse politie gebruikt bijvoorbeeld ANPR-camera's om kentekenplaten te analyseren. Deze camera's hebben enorme 'bijvangst' aan beelden uit de publieke omgeving, waaronder gezichten van automobilisten. Deze beelden gebruikte de politie vervolgens voor opsporingsdoeleinden.[84] In Rotterdam werden ANPR-camera's onrechtmatig gebruikt voor handhaving van de coronamaatregelen.[85] Daar reden in april 2020 politieauto's met ANPR-camera's om te controleren of mensen zich aan de anderhalfmeter afstand-maatregel hielden. Judith Veenkamp, hoofd van het Smart Citizens Lab bij Waag, noemde het "vooral opmerkelijk dat er in een crisissituatie totaal voorbij wordt gegaan aan de mogelijkheid om elkaar aan te spreken op de noodzaak tot afstand houden".[86] Ook de Autoriteit Persoonsgegevens waarschuwt dat tijden van crisis geen reden mogen zijn voor overheden om naar technologische middelen te grijpen zonder dat over alternatieven is nagedacht.[87]

81. De Vries, *Algoritmes en lokale overheden*, p. 57-61.
82. Beantwoording feitelijke/technische vragen van de fractie van D66: Algoritmes in organisatie Gemeente Leidschendam-Voorburg (1560), *Gemeente Leidschendam-Voorburg*, 16 oktober 2020.
83. H.E. Schild en M. Mulder, Beantwoording ex. Artikel 40 vragen algoritmes, *Gemeente Goes*, 2 december 2020, Z20.064662 / D20.698811, p. 2-3.
84. A. Herter, 'Tienduizenden mensen mogelijk onterecht in database politie', *NRC*, 16 maart 2021 geraadpleegd van https://www.nrc.nl/nieuws/2021/03/16/tienduizenden-mensen-mogelijk-onterecht-in-database-politie-a4035741.
85. A. Kouwenhoven, en M. Kuiper, Rotterdam schond privacy burgers met camera-auto's, *NRC*, 17 november 2021, geraadpleegd van https://www.nrc.nl/nieuws/2021/11/17/rotterdam-schond-privacy-burgers-met-camera-autos-a4065950.
86. Autoriteit Persoonsgegevens, *Smart Cities*, p. 28.
87. Autoriteit Persoonsgegevens, *Smart Cities*, p. 11.

Een ander risico bij slimme stad-toepassingen is excessieve dataverzameling. In de AVG is vastgelegd dat data alleen verzameld en bewaard mogen worden wanneer deze nodig zijn om het beoogde doel te bereiken. Dit wordt ook wel dataminimalisatie genoemd. Overheden houden zich hier lang niet altijd aan. Zo beschikt de Nederlandse politie over een gezichtsherkenningsdatabase genaamd Catch, waarmee ze foto's van nieuwe en bekende verdachten vergelijkt. In deze database werden tienduizenden foto's bewaard van mensen die niet meer verdacht werden.[88] Hoogleraar Rechtsgeleerdheid Joris van Hoboken zei hierover: "De overheid moet wel een legitieme reden hebben om op zo'n grote schaal dit soort gevoelige gegevens op te slaan. Het moet niet andersom zijn. Anders kom je in een controlestaat terecht."[89] Bij excessieve dataverzameling en het te lang bewaren van gegevens wordt volgens de hoogleraar de kans op privacy-schendingen groter.[90]
Incidenten met technologie schaden het vertrouwen van de burger in het toepassen van technologie door de overheid.[91] En het vertrouwen in de overheid is op moment van schrijven al relatief laag, blijkt uit cijfers van het Sociaal Cultureel Planbureau.[92] Meer democratische controle op technologische toepassingen betekent natuurlijk niet per definitie dat bij de toepassing meer oog is voor de belangen van inwoners.[93] Immers kunnen via een democratische weg ook besluiten genomen worden die leiden tot meer surveillance. Wel kunnen investeringen in het democratische gehalte van overheidsbesluiten bijdragen aan het voorkomen van onrecht.[94] Dit democratiseren kan beginnen bij het aanwakkeren van een inhoudelijk politiek debat over technologische toepassingen, in het bijzonder slimme stad-projecten. Het betrekken van inwoners bij besluiten kan hieraan een goede toevoeging zijn.

88. S. Hulsen, Tienduizenden mensen mogelijk onterecht in gezichtsdatabase van de politie, *NU.nl*, 16 maart 2022, geraadpleegd van https://privacy-web.nl/nieuws/gezichtendatabase-politie-mogelijk-onrechtmatig/.
89. Ibidem.
90. Ibidem.
91. T. Selbach en B. Brink, Hoe SyRI het belang van transparantie onderstreept, *Beleid en Maatschappij* 48, nr. 3 (2021): p. 3.
92. J. Den Ridder et al., *Burgerperspectieven 2021 | kwartaal 4* (Den Haag: Sociaal en Cultureel Planbureau, 2021), p. 4.
93. J. Himmelreich, Against "Democratizing AI", *AI & Society*, 2022, p. 10.
94. J. Himmelreich, Against "Democratizing AI", p. 2.

Digitale autonomie

§4

Digitale autonomie – de zeggenschap van overheden over data en technologie – staat hoog op de Europese politieke agenda. Steeds vaker zetten ook nationale overheden digitale autonomie op de politieke agenda. Deze paragraaf laat zien dat digitale autonomie ook een belangrijk streven is voor lokale bestuurders en politici. Ook gemeentebesturen kunnen namelijk de zeggenschap verliezen over wat er gebeurt met de data van inwoners.

Digitale autonomie is een afgeleide van strategische autonomie, een term die oorspronkelijk in de context van defensiebeleid werd gebruikt.[95] Zo omschrijft de Nederlandse Cyber Security Raad strategische autonomie als "het vermogen en de middelen om beslissingen te kunnen nemen en uit te voeren aangaande essentiële aspecten van de lange termijn-toekomst in economie, maatschappij en democratie".[96] Digitale autonomie is strategische autonomie op digitaal vlak.[97] Dit wil zeggen: de zeggenschap over data, software-standaarden en protocollen, processen, hardware, digitale diensten, en infrastructuur.[98]

Digitale autonomie is een term die veel wordt gebruikt binnen het Europese politieke debat. Politici bezigen de term vaak afwisselend met digitale en technologische soevereiniteit. Soevereiniteit op het niveau van een staat betekent het waarborgen van de legitimiteit van de staat ten opzichte van zowel andere landen (externe soevereiniteit) als inwoners (interne soevereiniteit).[99] Waar digitale of technologische soevereiniteit een doel is, is digitale autonomie een middel om dit te bereiken.[100] Met andere woorden: de mogelijkheid voor een staat om te beslissen over digitale zaken (digitale autonomie) is een manier om diens legitimiteit (digitale soevereiniteit) te kunnen behouden.

Digitale autonomie staat sinds de coronacrisis in toenemende mate op de Europese politieke agenda. De beslissingsruimte over digitale zaken van de Europese Unie staat onder druk, voornamelijk door een te afhankelijke positie voor de EU ten opzichte van de Verenigde Staten (VS) en China als het gaat om technologie.[101] De Europese Commissie maakt zich bijvoorbeeld zorgen over democratische uitholling door haatzaaierij en verspreiding van desinformatie via Amerikaanse sociale mediaplatforms zoals Facebook, Twitter en YouTube. Wetten om de grote sociale mediaplatforms te beteugelen, zijn in de maak, zoals de Wet inzake Digitale Diensten en de Wet inzake Digitale Markten.[102] De Dataverordening moet het delen van data tussen consumenten, bedrijven en overheden stimuleren, met in achtneming van de rechten van mensen. Met de Wet op de Artificiële Intelligentie wil de Europese Commissie kaders stellen voor het toepassen van kunstmatige intelligentie, ook door overheidsdiensten, en investeren in Europese AI-innovatie om de digitale autonomie te verstevigen.[103] De Europese Commissie maakt zich ook zorgen over de Europese afhankelijkheid voor de levering van halfgeleiders – essentieel voor producten zoals auto's en computers – vanuit de VS en China. De Europese Commissie wil daarom de productie opschroeven

95. L. Faesen et al., Soevereiniteit en Digitale Autonomie, *The Hague Centre for Strategic Studies* (2021): p. 3.
96. *CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity': Hoe verminderen we onze digitale afhankelijkheden met behoud van een open economie?* (Den Haag: Cyber Security Raad, 2021), p. 5.
97. Ibidem.
98. L. Floridi, The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU, *Philosophy & Technology*, 33 (2020): 369-378, p. 370-371.
99. J. Pohle en T. Thiel, Digital Sovereignty, *Internet Policy Review*, 9, nr. 4 (2020): p. 3.
100. Cyber Security Raad, *CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity'*, p. 5.
101. T. Madiega, Digital Sovereignty for Europe, *European Parliamentary Research Service* (2020): p. 1.
102. L. de Vries, J-J. Goeijenbier, en A. Groen, Wat staat er op het spel met nieuwe EU-regels voor Big Tech? *Idee* (2021): p. 70-75.
103. COM(2021) 206 final.

Gemeentebesturen kunnen de zeggenschap verliezen over wat er gebeurt met de data van inwoners.

zodat in 2030 twintig procent van de halfgeleiders in de EU wordt geproduceerd.[104] Een andere bron van zorg is de afhankelijkheid van de EU ten opzichte van de Verenigde Staten als het gaat om clouddiensten. Met de cloudinfrastructuur GAIA-X poogt de Europese Commissie de digitale autonomie van de EU op dit vlak te herstellen.[105]

Ook nationale overheden streven naar digitale autonomie. Dit geldt zowel voor democratische als niet-democratische landen. In China staat 'cyber soevereiniteit' sinds 2010 hoog op de nationale agenda.[106] China legt ook druk op landen in Afrika om te investeren in hun 'digitale soevereiniteit', waarbij China vooral hoopt de eigen invloed in deze landen te kunnen vergroten via het installeren van surveillancetechnologie.[107] Ook de weinig democratische Russische overheid heeft digitale autonomie hoog op de agenda staan.[108] Waar het beleid in China voor meer digitale soevereiniteit vooral gericht is op het vergroten van de macht van de nationale overheid – bijvoorbeeld door minderheden zoals de Oeigoeren met behulp van biometrie te discrimineren en onderdrukken – wil de Europese Commissie maatregelen voor meer digitale soevereiniteit op een mensgerichte manier vormgeven en in overeenkomst brengen met de 'Europese waarden'.[109] Of het EU-beleid voor meer digitale soevereiniteit in de praktijk strookt met deze waarden is voer voor discussie.[110]

Voor democratische nationale overheden is digitale autonomie eveneens een belangrijk thema geworden. Zo liet de Duitse regering in 2019 een onderzoek uitvoeren naar de digitale autonomie van het land. Uit dit onderzoek bleek een te grote afhankelijkheid van Microsoft voor digitale diensten.[111] Volgens de onderzoekers zou dit onder andere kunnen leiden tot minder toegang tot en vertrouwelijkheid van informatie en hogere kosten.[112] Ze waarschuwen ook voor juridische onzekerheid: niet altijd is namelijk duidelijk of diensten van leveranciers wel aan de AVG voldoen, vanwege gebrekkige transparantie.[113] In Nederland waarschuwde de Cyber Security Raad, een onafhankelijk nationaal adviesorgaan, in mei 2021 dat de digitale autonomie onder druk staat. Nederland zou te afhankelijk worden van enkele buitenlandse marktspelers voor de digitale infrastructuur, zoals clouddiensten.[114] Ook in de Tweede Kamer groeit de aandacht voor het thema. Lisa van Ginneken, Tweede Kamerlid voor D66, pleitte in september 2021 voor meer investeringen van de Nederlandse overheid in digitale soevereiniteit.[115]

104. Digital sovereignty: Commission kick-starts alliances for Semiconductors and industrial cloud technologies, *Europese Commissie*, 19 juli 2021, geraadpleegd van https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3733.
105. S. Autolitano en A. Pawlowska, Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study, *Instituto Affari Ineernazionali*, 21 (2021): p. 3.
106. R. Creemers, China's Conception of Cyber Sovereignty: Rhetoric and Realization, in *Governing Cyberspace: Behavior, Power, and Diplomacy*, red. D. Broeders en B. van den Berg (Landham: Rowman & Littlefield, 2020): 107-142, p. 2.
107. Y. Adegoke, The real reason China is pushing "digital sovereignty" in Africa, *Rest of World*, 1 december 2021, geraadpleegd van https://restofworld.org/2021/the-real-reason-china-is-pushing-digital-sovereignty-in-africa/.
108. Pohle en Thiel, Digital Sovereignty, p. 9.
109. The EU's capacity to act in a digital world, *Europese Commissie*, 26 mei 2021, geraadpleegd van https://ec.europa.eu/commission/commissioners/2019-2024/vestager/announcements/eus-capacity-act-digital-world_en.
110. H. Roberts et al., Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies, *Internet Policy Review*, 10, nr. 3 (2021): p. 18-20.
111. *Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern* (Berlijn: Strategy&, 2019), p. 3.
112. Ibidem, p. 7-8.
113. Ibidem, p. 18.
114. Cyber Security Raad, *CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity'*, p. 9.
115. R. van Houten, 'We moeten investeren in techsoevereiniteit', *iBestuur*, september 2021, geraadpleegd van https://ibestuur.nl/magazine/we-moeten-investeren-in-techsoevereiniteit.

Tot op heden is echter weinig aandacht voor digitale autonomie bij *lokale* overheden. Dit terwijl ook in gemeenten via de hierboven besproken slimme stad-projecten het risico op afhankelijkheid van (buitenlandse) bedrijven ontstaat. Gemeenten worstelen met een gebrek aan interne kennis en expertise op het gebied van digitalisering en technologie, het beperkte aantal private software-aanbieders om mee in zee te gaan bij ICT-projecten, en onduidelijkheid over wie zeggenschap heeft over data die worden verzameld. Dit maakt digitale autonomie ook voor gemeentebesturen tot een belangrijk vraagstuk. Hierbij speelt een aantal ontwikkelingen een rol.

Risico's van publiek-private samenwerkingen

Slimme stad-projecten zijn over het algemeen publiek-private samenwerkingen.[116] Risico's voor gemeenten zijn onder meer dat zij beperkte toegang hebben tot data, de belangen van inwoners uit het oog verliezen en taken gaan uitvoeren die niet bij de gemeente horen.

Het slimme stad-project Jouw Licht op 040 in Eindhoven is een voorbeeld van een project waar het misging en dat midden in de pilotperiode is stopgezet.[117] Bij dit project wilde de gemeente Eindhoven met Philips Lighting en het bedrijf Heijmans 'slimme' lantaarnpalen met bijvoorbeeld geluids- of bewegingssensoren plaatsen. Tijdens de samenwerking ontstond veel juridische onduidelijkheid. De partijen wisten niet wat de wettelijke verplichtingen precies waren, omdat bij de samenwerking zowel publieke als commerciële taken werden uitgevoerd. Philip Lighting en Heijmans voerden bij dit project bijvoorbeeld wel publieke taken uit, maar omdat zij geen overheidsdiensten zijn, waren zij niet wettelijk verplicht de data te delen. Voor de gemeente Eindhoven was het delen van de data echter een belangrijk speerpunt.[118] Ook was onduidelijk welke partij in het project aangewezen moest worden als dataverzamelaar.[119]

Een ander gevaar is dat de belangen van inwoners bij slimme stad-projecten over het hoofd worden gezien. Slimme stad-projecten brengen het risico met zich dat ze vooral gedreven worden vanuit de commerciële belangen van technologiebedrijven.[120] Dit wordt ook wel *corporate technology push* genoemd.[121] Het meest bekende voorbeeld hiervan is het Google Sidewalk Labs project in Toronto.[122] Het Canadese stadsbestuur wilde met het dochterbedrijf van Google genaamd Sidewalk Labs een living lab bouwen. Onderdeel van het living lab zou de app Replica zijn, waarmee geregistreerd zou worden wanneer, via welk vervoersmiddel en waarheen mensen zich bewegen.[123] Inwoners vreesden voor surveillancepraktijken door Google.[124] Onderzoekers noemen het project 'top-down' georganiseerd en 'technologie-gedreven'.[125] Het project is stopgezet, officieel vanwege de onzekere economische situatie die is ontstaan door het coronavirus.[126] Maar waarschijnlijk hebben de protesten van inwoners tegen het initiatief ook een belangrijke rol gespeeld bij het nemen van dit besluit.[127]

Een derde risico is dat gemeenten taken gaan uitvoeren die niet onder hun verantwoordelijkheid vallen. Zo biedt het bedrijf Pantyr met onder andere

116. Voorwinden, The Privatised City: Technology and Public-Private Partnerships in the Smart City, p. 444.
117. B. Karstens, L. Kool, en R. van Est, De slimme stad, grote beloften, weerbarstige praktijk, *Justitiële verkenningen*, 3 (2020): 10-23, p. 12.
118. Ibidem, p. 14-15.
119. Ibidem, p. 15.
120. L. van Zoonen, Publieke waarden of publiek conflict: democratische grondslagen voor de slimme stad, *Justitiële verkenningen*, 46, nr. 3 (2020): 51-64, p. 59.
121. A. Brem, K.I. Voigt, Integration of Market Pull and Technology Push in the Corporate Front and Innovation Management – Insights from the German Software Industry, *Technovation*, 29 (2009): 351-367, p. 355.
122. Van Zoonen, Publieke waarden of publiek conflict, p. 55.
123. N. Bowden, Introducing Replica, a next-generation urban planning tool, *Medium*, 6 april 2018, geraadpleegd van https://medium.com/sidewalk-talk/introducing-replica-a-next-generation-urban-planning-tool-1b7425222e9e.
124. L. Cecco, Toronto swaps Google-backed, not-so-smart city plans for people-centred vision, *The Guardian*, 12 maart 2021, geraadpleegd van https://www.theguardian.com/world/2021/mar/12/toronto-canada-quayside-urban- centre.
125. K. Morgan, en B. Webb, Googling the city, *Urban Planning and the Smart City: Projects, Practices and Politics*, 5, nr. 1 (2020): 84-95, p. 90.
126. Sidewalk Toronto, *Sidewalk Labs*, geraadpleegd op 8 maart 2022 van https://www.sidewalklabs.com/toronto.
127. Van Zoonen, Publieke waarden of publiek conflict, p. 55.

een digitaal dashboard een "totaaloplossing" aan voor een "integrale aanpak van ondermijning".[128] Pantyr biedt een app aan, genaamd Meld een Vermoeden, waarmee inwoners melding kunnen maken van verdachte situaties. De app wordt al in meer dan dertig Nederlandse gemeenten gebruikt. Volgens de Autoriteit Persoonsgegevens nemen gemeenten hiermee een taak over van de politie.[129] Daarnaast roept deze app vragen op over databeveiliging, hoe wordt omgegaan met bevooroordeelde meldingen en de wenselijkheid van de sociale controle die hiermee wordt gestimuleerd.[130] Bovendien lopen gemeentebesturen het risico de toegang te verliezen tot de data(-analyses), en daardoor het inzicht in wat er precies met de data van inwoners gebeurt.

Groeiende afhankelijkheid

Ook voor ICT-systemen zoals burgerapplicaties is sprake van een groeiende afhankelijkheid van gemeentebesturen ten opzichte van leveranciers. Door grote machtsconcentraties op de ICT-markt worden kleine aanbieders vaak opgekocht door grotere. Dit heeft ertoe geleid dat Nederlandse gemeenten voor een aantal ICT-diensten afhankelijk zijn van slechts een handvol aanbieders.[131] Er zijn vijf grote spelers op de ICT-markt voor gemeenten: Centric, Conxillium, MainCapital, TSS en Visma.[132] Deze machtsconcentratie vergroot voor gemeentebesturen de kans op vendor lock-in. Van *vendor lock-in* is sprake bij een grote mate van afhankelijkheid van een bedrijf voor het leveren van bepaalde diensten. Dit is bijvoorbeeld het geval wanneer gemeentebesturen een product of dienst afnemen van een (software)leverancier en vervolgens ook voor andere producten of diensten afhankelijk zijn van deze leverancier. Gemeenten staan dan voor de keuze: ofwel nog meer diensten van dezelfde leverancier aanschaffen, of overstappen naar een andere aanbieder. Dit laatste gaat meestal gepaard met hoge kosten. De afhankelijkheid van (software)leveranciers bij slimme stad-projecten vergroot de kans dat het gemeentebestuur voor langere tijd 'verstrikt' raakt in een contract.[133]

Om tegenwicht te bieden aan de macht aan van de software-aanbieders, moeten gemeenten hun krachten bundelen. Bijvoorbeeld door gezamenlijk nieuwe standaarden in te voeren voor het delen en inzichtelijk maken van data. Van samenwerking tussen gemeenten is in de praktijk nog te weinig sprake.[134] Er zijn enkele initiatieven, bijvoorbeeld vanuit de Vereniging van Nederlandse Gemeenten. Zij bieden met de zogenoemde Common Ground Principes gemeentebesturen handvatten om meer grip te krijgen op hun data. De steden Amsterdam, Barcelona en New York hebben de Cities Coalition for Digital Rights opgericht, waarbij ze met tientallen steden opkomen voor digitale rechten waaronder open digitale standaarden.[135]

Veel contracten die gemeenten sluiten met leveranciers zijn op abonnementsbasis. Deze diensten worden meestal aangeduid als 'as a service', zoals 'light as a service' en 'mobility as a service'. Er is SaaS (Software as a Service), PaaS (Platform as a Service), (IaaS Infrastructure as a Service) en DaaS (Database as a Service).[136] Het bedrijf dat is ingeschakeld voor de in §1 genoemde digital twin in Eindhoven noemt dit product bijvoorbeeld "Data-as-a-service".[137] De afnemer betaalt maandelijks of jaarlijks. De installatie en

128. Meld een Vermoeden ontvangt investering voor totaaloplossing criminaliteitsbestrijding, *Meld een Vermoeden*, geraadpleegd op 8 maart 2022 van https://www.meldeenvermoeden.nl/nieuws/meld-een-vermoeden-ontvangt-investering-voor-totaaloplossing-criminaliteitsbestrijding/.
129. J.F. van Wijnen, Gemeenten moedigen burgers aan om over elkaar te klikken via omstreden app, *Het Financieele Dagblad*, 16 augustus 2021, geraadpleegd van https://fd.nl/ondernemen/1407223/tientallen-gemeenten-gebruiken-klik-app-voor-burgers-en-ondernemers-lga2cap7YH3d.
130. L. de Vries, Willen we een samenleving waarin buren elkaar aangeven? *Het Financieele Dagblad*, 20 augustus 2021, geraadpleegd van https://fd.nl/opinie/1408466/willen-we-een-samenleving-waarin-buren-elkaar-aangeven- kla2cap7YH3d.
131. K. Groeneveld en H. Timmermans, *Reset de gemeentelijke ICT: Op zoek naar een evenwicht tussen zelf doen en uitbesteden* (Zaltbommel: Haystack, 2021), p. 55.
132. Ibidem, p. 72.
133. Voorwinden, The Privatised City: Technology and Public-Private Partnerships in the Smart City, p. 456.
134. Groeneveld en Timmermans, *Reset de gemeentelijke ICT*, p. 56.
135. Declaration of Cities Coalition for Digital Rights, Cities for Digital Rights, geraadpleegd van https://citiesfordigitalrights.org/assets/Declaration_Cities_for_Digital_Rights.pdf, p. 2.
136. Groeneveld en Timmermans, *Reset de gemeentelijke ICT*, p. 253.
137. 3D Digital Twin – Eindhoven, Argaleo, Geraadpleegd op 3 maart 2022 via: https://www.youtube.com/watch?v=9v-_iUd9Kp8.

het beheer van de toepassing worden meestal gedaan door de aanbieder. Op deze manier zouden gemeenten volledig worden "ontzorgd".[138] Met deze abonnementen zitten gemeenten niet met hoge aanschafkosten en kunnen ze de dienst maandelijks aanpassen. Dit geldt echter ook voor de leverancier van de dienst, wat weer onzekerheid creëert voor gemeentebesturen.

Niet altijd is duidelijk wat bedrijven precies doen met de data die worden verzameld bij slimme stad-projecten. Data – of analyses van de data – kunnen bijvoorbeeld worden verkocht aan andere bedrijven. Bij doorverkopen is amper nog zicht op wat er met de data gebeurt.[139] En niet alleen bij doorverkopen, maar ook bij het hergebruiken van data kunnen privacyschendingen ontstaan, zelfs als deze data geen persoonsgegevens bevatten. In combinatie met andere datasets kan het alsnog mogelijk zijn om gevoelige persoonsgegevens te genereren.[140] Ook het combineren van openbare databronnen kan de privacy schenden.[141] Belangrijk is dus niet alleen welke data bedrijven verzamelen, maar ook wat hiermee gebeurt.

Box 5. Camera's van Hikvision en Dahua

Een aantal ministeries en enkele gemeenten, waaronder Amsterdam, Lelystad, Zoetermeer en Schiedam, gebruiken camera's van de bedrijven Hikvision en Dahua.[142] Dit zijn Chinese bedrijven van wie camera's ook gebruikt worden door de Chinese overheid voor de onderdrukking van de Oeigoerse bevolking in Xinjiang. Het gebruiken van deze camera's roept niet alleen vragen op over databeveiliging van digitale infrastructuur, maar ook over de wenselijkheid om producten van een bedrijf te gebruiken dat betrokken is bij mensenrechtenschendingen.[143] De Chinese overheid zet technologische toepassingen zoals camera's in andere landen in om met de verzamelde data de software van producten te kunnen verbeteren.[144] Dit zou weleens kunnen betekenen dat ook de data die worden opgevangen via camera's in Nederland worden gebruikt voor verbetering van Chinese onderdrukkingssoftware.

138. R. Bartels, *Gemeenten ontzorgd met SaaS: Software as a Service voor de decentrale overheid* (Centric Public Sector Solutions, 2021), p. 1.
139. V. Chang, An Ethical Framework for Big Data and Smart Cities, *Technological Forecasting and Social Change*, 165 (2021), p. 8.
140. Karstens, Kool, en Van Est, De slimme stad, grote beloften, weerbarstige praktijk, p. 17.
141. C. Metz en K. Hill, Here's a Way to Learn if Facial Recognition Systems Used Your Photos, *The New York Times*, 31 januari 2021, geraadpleegd van https://www.nytimes.com/2021/01/31/technology/facial-recognition-photo-tool.html.
142. J. Schellevis en T. Spekschoor, Omstreden Chinese camera's hangen overal in Nederland, ook bij ministeries, *NOS*, 8 februari 2022, geraadpleegd van https://nos.nl/artikel/2416279-omstreden-chinese-camera-s-hangen-overal-in-nederland-ook-bij-ministeries.
143. S. Eikelenboom en S. Brommersma, Nederlandse Overheid weet niet dat ze op grote schaal Chinese camera's gebruikt, *Follow the Money*, 1 maart 2022, geraadpleegd van https://www.ftm.nl/artikelen/overheid-ontbeert-inventaris-hikvision-dahua.
144. A. Hawkins, Beijing's Big Brother Tech Needs African Faces: Zimbabwe is Signing up for China's Surveillance State, but its Citizens will Pay the Price, *Foreign Policy*, 24 juli 2018, geraadpleegd van https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/.

'Slim' of 'geprivatiseerd'?

Wetenschappers en experts waarschuwen al jaren voor groeiende afhankelijkheid van overheden van de private sector bij slimme stad-projecten. In 2016 zei onderzoeker en publicist Evgeny Morozov al dat "de levering van essentiële diensten – ooit louter de bevoegdheid van de verzorgingsstaat en lokale overheden – afhangt van de nukken van bedrijven en hun bedrijfsmodellen."[145] De stad is volgens hem "het voornaamste doelwit van Big Tech".[146] 'Slim' betekent volgens hem in de praktijk meestal 'geprivatiseerd'. De uitvoering van overheidstaken, zoals vervoer, (digitale) infrastructuur, criminaliteitsbestrijding, worden door slimme stad projecten steeds meer uit handen gegeven aan de private sector. Met als gevolg een overheid die grip verliest op haar diensten en de data die met het uitvoeren van die diensten verzameld worden.

Dit risico neemt toe door het in toenemende mate uitbesteden van publieke diensten aan private partijen. Sinds de jaren 90 is een trend gaande, waarbij de overheid essentiële diensten uitbesteed aan bedrijven "die hun werk bedrijfsmatig doen, waarbij de burger een klant is die binnen de productdoelstellingen moet vallen".[147] De afgelopen jaren is het uitbestedingspercentage van gemeenten bovendien flink toegenomen. Waar in 2016 nog 16 procent van de gemeentelijke software werd uitbesteed aan leveranciers, was dit in 2020 gestegen naar 35 procent. Naar verwachting zal dit percentage in 2025 liggen op 60 procent.[148] Gemeenten kochten in totaal voor 41,5 miljard euro per jaar in. Dit is bijna het dubbele van het bedrag aan uitbestede diensten van de landelijke overheid, namelijk 22,3 miljard euro.[148] Door dergelijke diensten uit te besteden, hoeven gemeenten niet de – meestal dure – kennis in huis te halen voor de ICT-toepassingen die onderdeel zijn van slimme steden. Uit een vragenlijst onder 117 managers en leidinggevenden bij gemeenten bleek dat 63 procent van mening is dat bestuurders te weinig kennis hebben van ICT.[150] Deze financiële overweging is begrijpelijk, maar niet zonder consequenties. Door ICT-processen uit te besteden aan externe partijen, vindt namelijk een "onnodige versnippering van kennis, capaciteit en middelen" plaats.[151] Het uitbesteden van ICT-diensten houdt het gebrek aan kennis binnen de gemeente in stand.

Uitbesteding van overheidstaken aan de private sector is echter niet per definitie slecht, zolang deze maar is gericht op het publieke belang, zo betoogt hoogleraar economie Mariana Mazzucato.[152] Volgens haar kunnen juist publiek-private samenwerkingen de grote maatschappelijke uitdagingen van deze tijd, zoals klimaatverandering, ontoegankelijkheid van de gezondheidszorg, en sociale en economische ongelijkheid, aanpakken.[153] Toch hebben bedrijven niet dezelfde belangen als overheden en bovendien niet dezelfde democratische legitimiteit.[154] Uitbesteding hangt daarnaast mogelijk samen met een lagere tevredenheid van inwoners over overheidsdiensten.[155] Gemeentebesturen moeten daarom duidelijke afspraken maken met bedrijven over wat zij wel en niet mogen doen met data van inwoners, en investeren in het democratische gehalte van slimme stad-toepassingen.

---

145. E. Morozov, Only a Cash-Strapped Public Sector Still Finds 'Smart' Technology Sexy, *The Guardian,* 11 september 2016, geraadpleegd van https://www.theguardian.com/commentisfree/2016/sep/10/only-public-sector-finds-smart-technology-sexy.
146. E. Morozov, We Sharen Van Alles Behalve de Macht, *NRC*, 23 augustus 2018, geraadpleegd van https://www.nrc.nl/nieuws/2018/08/23/we-sharen-van-alles-behalve-de-macht-a1614026?t=1640010874.
147. T- J. Meeus, Talrijke Miljarden voor een Overheid wier Gezag en Expertise Uitgehold zijn, *NRC*, 18 december 2021, geraadpleegd van https://www.nrc.nl/nieuws/2021/12/18/talrijke-miljarden-voor-een-overheid-wier-gezag- en-expertise-uitgehold-zijn-2-a4069445?t=1639904111.
148. ICT Benchmark Gemeenten 2021, *M&I/Partners*, geraadpleegd op 14 maart 2022 van https://mxi.nl/uploads/files/page/ict-benchmark-gemeenten-2021-conclusies.pdf, p. 18.
149. R. van Weert et al., Het Inkoopvolume van de Nederlandse Overheid, *Significant*, 15 september 2016, geraadpleegd van https://www.pianoo.nl/sites/default/files/documents/documents/inkoopvolume-van-nederlandse-overheid-september2016.pdf, 27.
150. Veranderbesef moet leiden tot veranderbereidheid: Het Digitale OverheidsOnderzoek: Gemeente 2030, *BCT*, 2021, geraadpleegd van https://www.bctsoftware.com/nl/het-digitale-overheidsonderzoek-gemeente-2030/, p. 14.
151. Groeneveld en Timmermans, *Reset de gemeentelijke ICT*, p. 2.
152. Mazzucato, *Mission Economy*, p. 23.
153. Mazzucato, *Mission Economy*, p. 105-159.
154. Passchier, *AI en de Rechtsstaat*, p. 55-56.
155. C. Dahlström, M. Nistotskaya, en M. Tyrberg, Outsourcing, bureaucratic personnel quality and citizen satisfaction with public services, *Public Administration*, 96, nr. 1 (2018): p. 18.

Box 6. Toekomsttechnologie: het voorbeeld van drones

De toepassing van nieuwe technologieën in gemeenten en steden zal waarschijnlijk alleen maar toenemen. De WRR noemt kunstmatige intelligentie ook wel een nieuwe 'systeemtechnologie', vergelijkbaar met de ontwikkeling van elektriciteit.[156] Nieuwe toepassingen zoals het inzetten van drones voor niet-militaire doeleinden in steden zullen naar verwachting de komende decennia een enorme vlucht nemen.[157] De Nederlandse politie gebruikt bijvoorbeeld al drones voor *crowd control*.[158] Ook kunnen drones worden toegerust met warmte- en geluidssensoren en camera's voor gezichtsherkenning. Amazon is bezig met het ontwikkelen van drones voor pakketbezorging.[159] Dit zal nieuwe vragen oproepen: over privacy, veiligheid, verantwoordelijkheid, en werkgelegenheid.[160] Het maakt een politiek debat over technologische inzet in steden nog noodzakelijker. De vraag in hoeverre gemeentebesturen afhankelijk zijn van private partijen voor digitale diensten zal een onderdeel moeten zijn van dit debat.

156. Prins et al., *Opgave AI*, p. 12.
157. What is Urban Air Mobility? *European Union Aviation Safety Agency*, geraadpleegd op 7 maart 2022 van https://www.easa.europa.eu/what-is-uam.
158. Zo schat de politie in hoeveel mensen er op een demonstratie komen, *NOS*, 9 september 2021, geraadpleegd van https://nos.nl/artikel/2397182-zo-schat-de-politie-in-hoeveel-mensen-er-op-een-demonstratie-komen.
159. First Prime Air Delivery, *Amazon*, 7 december 2016, geraadpleegd van https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011.
160. R. Kellermann en L. Fischer, Drones for parcel and passenger transport: A qualitative exploration of public acceptance, *Sociología y Tecnociencia*, 10, nr. 2 (2020), 106-138, p. 114-130.

Conclusie

Gemeenten en steden maken volop gebruik van nieuwe technologieën om grote uitdagingen, zoals klimaatverandering, sociale en economische ongelijkheid en onveiligheid, het hoofd te bieden. In zogeheten smart cities (slimme steden) worden technologieën in de openbare ruimte – zoals meters, camera's en sensoren – ingezet om bijvoorbeeld luchtvervuiling en biodiversiteit te meten, gewelddadig gedrag op straat te signaleren of verkeersbewegingen te analyseren. Dit brengt volop kansen met zich, maar ook risico's. Dit paper biedt een sociaal-liberale uiteenzetting van drie principes die onder druk worden gezet door slimme stad-toepassingen: het gelijkheidsbeginsel, democratische controle en digitale autonomie.

§1 laat zien dat het gelijkheidsbeginsel in slimme stad toepassingen onder druk kan komen te staan. Sommige biometrische software is ontwikkeld op basis van data van enkel witte mensen, waardoor toepassingen minder betrouwbaar zijn op data van zwarte mensen. Dit kan discriminatie in de hand werken en sociale ongelijkheid versterken. Daar komt bij dat aan slimme stad-toepassingen vrijwel niet te ontkomen is omdat ze zich in de directe leefomgeving van inwoners bevinden. Bovendien kunnen biometrische toepassingen zoals gezichtsherkenningssoftware in slimme steden grote inbreuk doen op de individuele autonomie en keuzevrijheid van mensen. Experimenten met slimme stad-toepassingen mogen niet leiden tot experimenten met de rechten en vrijheden van inwoners.

Ten tweede kan democratische controle onder druk komen staan door slimme stad-toepassingen. Toepassingen met digitale technologieën in gemeenten staan lang niet altijd voldoende op de lokale politieke agenda. Dit komt onder andere doordat bestuurders en politici digitalisering als een kwestie voor de gemeentelijke uitvoering zien in plaats van als een onderwerp voor op de politieke agenda. Bovendien hebben gemeentebesturen en -raden niet altijd voldoende inzicht in de private software die gebruikt wordt bij slimme stad-toepassingen. Dit bemoeilijkt de controle op deze toepassingen door lokale bestuurders en politici. Politieke aandacht voor digitalisering en slimme steden is geen garantie voor eerlijk en rechtvaardig technologiegebruik, maar wel een noodzakelijke voorwaarde.

Het derde principe dat bij slimme stad-toepassingen onder druk kan staan is digitale autonomie. Doordat gemeentebesturen niet altijd voldoende grip hebben op wat er met de data van inwoners gebeurt, is de kans op datalekken en mensenrechtenschendingen door slimme stad-toepassingen groter. De publiek-private samenwerkingen in slimme steden brengt bovendien het risico met zich mee dat de belangen van inwoners uit het oog worden verloren. Dit schaadt ook het vertrouwen van inwoners in digitale toepassingen van de overheid. Herstel van grip op de digitale stad zou daarom prioriteit moeten hebben in de komende raadsperiode.

APK voor digitale autonomie in de slimme stad

Met onderstaande APK kunnen gemeentebesturen democratische grip herwinnen op slimme stad-toepassingen. De keuring is deels geïnspireerd door het boek *Reset de gemeentelijke ICT* van Kees Groeneveld en Herman Timmermans, waarin zij enkele voorstellen doen voor gemeenten om hun positie ten opzichte van (software)leveranciers in kaart te brengen.[161] Gemeenten en steden moeten de vruchten kunnen plukken van technologische ontwikkelingen, zodat slimme steden de vrijheid en mogelijkheden van inwoners vergroten, en tegelijkertijd de grote uitdagingen van deze tijd kunnen aanpakken.

1. De gemeenteraad heeft een raadscommissie Digitale Zaken.
2. Het college heeft een wethouder met de portefeuille Digitale Zaken.
3. Het college heeft een openbaar overzicht van alle slimme stad-toepassingen, waarin zij ook toelicht welke data door welke partijen worden verzameld, en met welk doel.[162]
4. Het college heeft voor elk van deze toepassing een Data Protection Impact Assessment uitgevoerd, en deze gedeeld met de gemeenteraad.
5. Het college heeft een openbaar sensorenregister.[163]
6. Het college heeft een openbaar algoritmeregister.
7. Het college laat jaarlijks een audit uitvoeren door een onafhankelijke organisatie op de software en digitale infrastructuur die onderdeel zijn van slimme stad-toepassingen.
8. Het college heeft een overzicht van de contracten die zijn afgesloten in het kader van slimme stad-projecten en met welke bedrijven, en deze gedeeld met de gemeenteraad.
9. Het college heeft een overzicht van contracten die zijn afgesloten met bedrijven in het kader van slimme-stad toepassingen en die op abonnementsbasis zijn, gedeeld met de gemeenteraad.

161. Groeneveld en Timmermans, Reset de gemeentelijke ICT, p. 205-209.
162. Onder slimme stad-projecten vallen alle projecten waarbij gebruik wordt gemaakt van digitale technologie in de openbare ruimte, zoals meters, camera's en sensoren.
163. Dit kan ook door deel te nemen aan het Sensorenregister van het Kadaster.

10 Het college heeft in de contracten met bedrijven in het kader van slimme stad-toepassingen vastgelegd dat zij toegang heeft tot alle verzamelde data.

11 Het college heeft duidelijke afspraken gemaakt over wat bedrijven in het kader van slimme stad-toepassingen wel en niet mogen doen met de verzamelde data.

12 Het college heeft bij de inkoop van slimme stad-toepassingen de exit-strategie vastgelegd, en deze gedeeld met de gemeenteraad.

13 Het college heeft vereisten voor technische en procedurele transparantie en uitlegbaarheid vastgelegd in de contracten met softwareleveranciers.[164]

164. Met als voorbeeld de voorwaarden voor transparantie ontwikkeld door de gemeente Amsterdam, zie: https://www.amsterdam.nl/innovatie/algoritmen-ai/contractvoorwaarden-algoritmen/.