

Ook in Nederland wordt dwangmatig gewerkt aan de digitale heilstaat

Posted on 8 september 2021 by Bina Ayar

Veilig contactloos betalen, veilig in de *cloud*. Het idee dat digitaal gelijk staat aan veiligheid is voor bedrijven en overheid een wet van Meden en Perzen. Opvallend is dat diezelfde partijen in digitalisering nu ook vaker gevaren zien. Toenemende afhankelijkheid van digitale technologie brengt veiligheidsrisico's met zich mee, denkt ook het demissionaire kabinet RutteDrie dat flink investeert in *cybersecurity*.

Naast veiligheidsrisico's levert doorgeslagen digitalisering ethische bezwaren op, zoals de opkomst van de controlemaatschappij en ontmenselijking. Grote afwezige in alle digitaliseringsdiscussies zijn de burgers. In de digitale heilstaat trekt de burger aan het kortste eind.

Vertrouwde techniek als terugvaloptie

In de jaren zeventig van de vorige eeuw verrijzen er nog altijd dieselgemalen in het land. Elektrische aandrijving van gemalen is dan de norm, maar via de Wet Bescherming Waterstaatswerken in Oorlogstijd (BWO) levert een dieselmotor

subsidie op.

Het idee achter de regeling is simpel: te grote afhankelijkheid van stroom vermijden, voor het geval de Russen aanvallen. Achteraf is er veel af te dingen op de wet, al helemaal omdat de Russische beer niet kwam, maar het idee om terug te vallen op oude, vertrouwde techniek is niet gek.

Digitale ontwrichting dreigt

Tegenwoordig hebben we steeds minder terugvalopties, constateert ook de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) in een rapport uit 2019 over digitale ontwrichting. Analoge alternatieven verdwijnen veelal of organisaties besteden belangrijke voorzieningen uit aan derde partijen.

Door de grote verwevenheid van de digitale en fysieke wereld loert volgens de raad het gevaar van digitale ontwrichting; het normale maatschappelijke leven waarin mensen stroom hebben, ziekenhuiszorg krijgen of bij hun geld kunnen, raakt ontwricht. Niet alleen door kwaadaardige aanvallen, maar ook door softwareproblemen, kapotte servers of andere digitale defecten. Een klein voorproefje daarvan kreeg de Nederlandse bevolking toen in 2019 alle alarmnummers ineens urenlang niet bereikbaar waren.

Cybersecurity is ook een prioriteit van het kabinet, zo blijkt uit de recente reactie van de minister van Justitie en Veiligheid op de WRR-aanbevelingen. Verschillende departementen gaan daarom mogelijke blinde vlekken in het ‘landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden’ inventariseren. Ook zal er vaker worden geoefend met ‘digitale branden’.

Aanvullende maatregelen om cyberschade te verzekeren zijn volgens het kabinet onnodig, omdat schade na cyberincidenten steeds vaker onder normale bedrijfspolissen valt en er vaker cyberpolissen worden aangeboden. Voor digitale veiligheid is 95 miljoen euro gereserveerd. Aan het brede publiek wordt ook gedacht: via educatiecampagnes en structurele voorlichting worden burgers ‘geïnformeerd over digitale risico’s’.

Burgers buiten beeld

Of de burger enige notie heeft van die gevaren valt te betwijfelen. Als het om cybersecurity gaat, blijven burgers buiten beeld, constateren ook Bernold Nieuwesteeg, directeur van het *EUR-instituut* *Centre for the Law and Economics of Cyber Security* en consultant Melle van den Berg, in een essay in *Binnenlands Bestuur*. Cybersecuritybeleid richt zich vooral op samenwerking tussen bedrijven en overheden, aldus de auteurs.

'Als we de cynische bril opzetten, dan komt de innige publiek-private samenwerking beide partijen erg goed uit. Belangrijk voor burgers is om te weten welke risico's zij moeten vrezen. Interessant is ook het antwoord op de vraag hoeveel belastinggeld er wordt besteed aan cybersecurity en of dat in verhouding staat met de risico's die burgers lopen.'

Maar burgers vertrouwen het niet

Waar burgers wel bekender mee zijn geraakt is het gebruik van algoritmes door gemeenten, toont onderzoek van KPMG. Nog geen twee op de tien Nederlanders heeft daar vertrouwen in, zo blijkt. Tachtig procent vindt dan ook dat er toezicht moet zijn op een verantwoord algoritmegebruik. Ruim veertig procent vindt dat het toezicht op het gebruik door de overheid strenger moet zijn dan op het gebruik door het bedrijfsleven.

De sceptische burger weet zich gesterkt door de Algemene Rekenkamer die in haar laatste rapport stelt dat de Rijksoverheid te weinig oog heeft voor de ethische aspecten van algoritmegebruik. Pijnlijke voorbeelden daarvan zijn de toeslagenaffaire en *SyRI* – een systeem dat poogde uitkeringsfraude tegen te gaan, maar strijdig bleek met het Europees Verdrag voor de Rechten van de Mens (EVRM).

Gezichtsherkenning verbieden?

Ook de wildgroei aan digitale middelen die het publiek coronaveilig moeten houden – van apps tot big data-surveillancesystemen en digitale vaccinatiepaspoorten- staan op gespannen voet met rechten van burgers. *Function creep*, het gebruik van technologie voor andere doeleinden dan oorspronkelijk bedoeld, is sinds de coronacrisis een werkwoord.

Niet voor niets pleit de Europese koepel van privacy toezichthouders voor een volledig verbod van elke vorm van gezichtsherkenning in de openbare ruimte en andere vormen van het verzamelen van biometrische gegevens; volgens de privacy waakhond een bedreiging voor de open, vrije samenleving.

Is digitalisering comfort of stress?

Het dagelijkse leven is evenmin makkelijker geworden door automatisering. Naast voordelen levert de *Do-it-yourself*-maatschappij stress op. Waar je vroeger bij anderen terecht kon voor informatie of diensten moet de *homo digitalis* alles zelf uitzoeken. Arbeidsdeling, een component van welvaart, lijkt daarmee eveneens in het geding.

Financieel wordt de gemiddelde Nederlander ook niet per se beter van digitalisering. Zo zijn dankzij de digitalisering van het geldverkeer burgers afhankelijk van banken die nu – dankzij ECB-beleid – zelfs negatieve rente berekenen voor spaargeld, of kosten rekenen voor geld pinnen. Wie te veel te koop loopt met afwijkende meningen loopt sinds kort zelfs het risico om helemaal te worden afgesloten van zijn bankrekening.

Hoewel digitalisering democratisering kan bevorderen, lijkt in de praktijk een klein clubje techmiljardairs in samenspraak met overheden en grote bedrijven de dienst uit te maken. De burger die veiligheid en meer vrijheid was beloofd, verandert in een wandelende streepjescode en raakt bovendien uit beeld.

Een van de ongewenste nadelige gevolgen van de alsmaar toenemende toepassing van bijvoorbeeld kunstmatige intelligentie (AI) kan volgens kennisinstituut TNO 'ontmenselijking' zijn – het gebruik van datasets maakt het makkelijker om de burger op afstand te houden.

Rotterdam: dwangmatige digitalisering

Desondanks wordt er gestaag doorgebouwd aan de digitale heilstaat. Het hart daarvan ligt in Rotterdam. De havenstad heeft de ambitie om digitale voorbeeldstad 2025 te worden. Met andere Europese steden tekende Rotterdam een convenant (via de site van de gemeente niet te raadplegen omdat de link niet werkt) waarin staat dat digitalisering een mensenrecht is.

De stad die in de woorden van dichter Jules Deelder te echt was om te filmen, bouwt aan een 3D-model van heel Rotterdam waarin alle objecten, van huizen, bomen tot bankjes, zijn opgenomen, aangevuld met live data over het gebruik. Rotterdammers kunnen verder bijvoorbeeld rekenen op experimenten met 'slimme' lichtmasten die worden uitgerust met 5G-antennes of camera's, en sensoren in de stad ('Hoe fijn zou het zijn als u altijd uw vuilniszak kwijt kunt in de ondergrondse container?').

Verder worden ook fietsers – geanonimiseerd – gevolgd met een camerasysteem. Volgens de verantwoordelijke GroenLinkswethouder is dat nodig omdat er geen volgsysteem was voor langzaam verkeer. Inzicht in hoe de Rotterdamse fietser zich verplaatst is belangrijk voor 'beleid'.

Veiligheid blijkt veiligheidsrisico

Enigszins geruststellend is, dat overheden wel nadenken over ethische bezwaren van doorgeslagen digitalisering. Daarbij klinkt steeds vaker de oproep van experts binnen en buiten de overheid tot een breed maatschappelijk digitaliseringsdebat.

Nu veiligheidssystemen zelf een veiligheidsrisico blijken en de coronacrisis – na anderhalf jaar afhaalmaaltijden, online onderwijs en verregaande controle voor schijnveiligheid – de grenzen aan digitalisering zichtbaar heeft gemaakt is de tijd rijp. Bij zo'n debat hoort ook het in twijfel trekken van het dogma dat digitaal altijd veiliger is of daarom beter. Voor bedrijven en overheden betekent dat tevens niet altijd toegeven aan controlezucht en datahonger. Dat vergt niet alleen wilskracht, maar ook wijsheid.