MINERVA
progressieve
denktank

Privacy in tijden van corona: hoe vermijden we algoritmische onderwerping?

Louis Mosar
april 2020

Minerva Paper 2020/03

Privacy in tijden van corona: hoe vermijden we algoritmische onderwerping?

Louis Mosar

In een poging om het covid-virus in te dijken, wordt ook gekeken naar de mogelijkheden van 'track and trace'-technologie, waarbij men via telefoongegevens de bewegingen van de bevolking traceert. Leidt dit inderdaad tot een versterking van de controlestaat, en komt onze privacy in gevaar?

In deze bijdrage verheldert Louis Mosar de vraag: het probleem is niet het verlies van privacy op zich, maar wel dat dit verlies van privacy tot dominantie en daardoor een verlies van vrijheid kan leiden. De algoritmes die bedrijven op basis van de verzamelde data ontwikkelen, bepalen in toenemende mate de kansen die mensen krijgen, maar zijn zelf niet controleerbaar en niet contesteerbaar.

Louis Mosar is filosoof en lid van Denktank Minerva.

e-mail: louis.mosar@gmail.com

Citeer als: Louis Mosar (2020), 'Privacy in tijden van corona: hoe vermijden we algoritmische onderwerping?' *Minerva Paper* 2020/03. Brussel: Denktank Minerva.

Privacy in tijden van corona: hoe vermijden we algoritmische onderwerping?

In de strijd tegen corona wordt lustig gebruik gemaakt van zogenaamde '*track-and-trace*'-technologie, waarbij men via telefoongegevens de beweging van de bevolking traceert om de verspreiding van het virus in kaart te brengen.[1] Dergelijke maatregelen zijn reeds in verschillende landen van kracht, waaronder China, Zuid-Korea, Polen en Israël. Ook in ons land is de overheid er al mee bezig. Sinds 11 maart verstrekken de telecomoperatoren data aan onze overheid en minister van Digitale Agenda Philippe De Backer richtte de taskforce 'Data against Corona' op. Deze taskforce werkt aan de ontwikkeling van strategieën om via het gebruik van *big data* de verspreiding van het virus in de kiem te smoren.

Mogelijks leidt dit tot een toename van de controlestaat, waarschuwen sommige analisten, zoals privacy-expert en activist Matthias Dobbelaere-Welvaert[2] en Israëlisch historicus Yuval Noah Harari.[3] Anderen, zoals Maarten Boudry, werpen tegen dat dit getuigt van 'obsessief piekeren over privacy', dat naar 'narcisme' neigt[4] (in een aanverwante context sprak Boudry in een opiniestuk uit 2014 over 'postmodern narcisme'[5]). Om een oordeel te vellen over de wenselijkheid van dergelijke maatregelen zijn de details en de concrete invulling cruciaal. Zo lijkt de app die in Zuid-Korea gangbaar is minder indringend dan die in China.[6] Eveneens is het belangrijk om duidelijkheid te scheppen over wat moderne *big data* surveillancetechnologie net zo problematisch maakt. Het is hier dat het huidige publieke debat tekortschiet. Het grote probleem is niet privacy op zich maar wel dat het verlies van privacy tot (anonieme) dominantie en daardoor tot een verlies van vrijheid leidt.

Privacy-narcisme, dominantie en vrijheid

Het debat wordt geframed als een debat over privacy *an sich*. Hoewel privacy *an sich* een legitieme bezorgdheid is (zoals het recente schandaal bij Google illustreert, waar medewerkers mee luisterden naar audiofragmenten die Google Assistant opnam[7]), dreigen we het echte probleem met *big data* en surveillancetechnologie op die manier te miskennen. Als het enige waarover we ons zorgen maken is dat vreemden naar onze persoonlijke gesprekken luisteren, dan heeft Maarten Boudry een punt om dit 'narcisme' te noemen. Bovendien wordt heel wat informatie tegenwoordig anoniem verwerkt en krijgt men vaak niet de persoonlijke informatie van anderen te zien of weet men niet welke informatie met naam en toenaam bij welke persoon hoort. Het probleem is in eerste instantie dan ook niet dat anderen je kleine en duistere geheimen kunnen bekijken of beluisteren, maar wel dat het prijsgeven van die informatie kan leiden tot een situatie van dominantie door overheid of bedrijven, zelfs als dat anoniem gebeurt via algoritmes.

> ***Het grote probleem is niet het verlies van privacy op zich, maar wel dat het verlies van privacy tot dominantie en daardoor tot een verlies van vrijheid leidt.***

Volgens filosoof Philip Pettit wordt iemand gedomineerd wanneer die persoon onderhevig is aan de *willekeurige* machtsuitoefening van één ander persoon of een groep personen.[8] We kunnen van willekeurige machtsuitoefening spreken wanneer iemand geen controle heeft over de macht die over hem/haar uitgeoefend wordt. Daardoor is deze machtsuitoefening niet verplicht om rekening te houden met de belangen van het gedomineerde individu. Het is makkelijk in te beelden dat het ontfutselen van bepaalde informatie kan leiden tot willekeurige machtsuitoefening. Stel je voor dat een hacker toegang krijgt tot het mailverkeer van een man die zijn vrouw bedriegt. Op dat moment kan de hacker de man domineren door te dreigen de informatie aan de vrouw vrij te geven als de man niet doet wat de hacker verwacht. De man bevindt zich in een ongelijke machtssituatie ten opzichte van de hacker en is volledig afhankelijk van diens willekeur. De hacker bepaalt volledig de termen van de verhouding tussen de hacker en de man, de laatste heeft geen controle over hun betrekking.

Wanneer mensen zoals Matthias Dobbelaere-Welvaert en Harari stellen dat als we onze persoonlijke gegevens aan de overheid afstaan, dit de deur openzet voor overheden om ons gedrag te voorspellen en te manipuleren, dan gaat dit ook over een bezorgdheid omtrent dominantie eerder dan over een bezorgdheid om wie al dan niet naar onze persoonlijke geheimen meeluistert. Zo kan het prijsgeven van op het eerste gezicht onbelangrijke informatie leiden tot het voorspellen en manipuleren van individueel gedrag, iets waar bedrijven reeds gebruik van maken. Denk bijvoorbeeld aan het Cambridge Analytica-schandaal, waarbij men via het verzamelen van Facebook-likes, consumentengedrag en internetgedrag, kiezersgedrag trachtte te manipuleren.[9]

Voor veel mensen zal het er waarschijnlijk weinig toe doen dat iemand anders weet naar waar je surft of wat je liket. Wat kan het je immers schelen dat een vreemde weet dat je Hello Kitty leuk vindt of dat een bepaalde seksuele fetisj spreekt uit je surfgedrag? De meeste mensen zullen dan weer wel aanstoot nemen aan manipulatie via het gebruik van deze data. Net zoals in het

voorbeeld van de hacker creëert dit een situatie waarin een instantie macht over ons kan krijgen waarover we geen controle hebben, een macht die niet ter verantwoording kan geroepen worden. Deze machtsuitoefening gebeurt achter onze rug en zonder dat we het beseffen. Privacy is dus geen doel op zich maar een noodzakelijke voorwaarde om vrijheid, gedefinieerd als de afwezigheid van dominantie, te verwezenlijken.

Privacy is geen doel op zich, maar een noodzakelijke voorwaarde om vrijheid te verwezenlijken.

Anonieme dominantie via '*weapons of math destruction*'

Het grote probleem is hier niet dat anderen directe toegang zouden hebben tot onze persoonlijke gegevens om ons, naar analogie met de hacker, op collectieve schaal af te persen. Ook wanneer gegevens volledig geanonimiseerd zijn en geen enkel mens directe toegang heeft tot je individuele data, kan dominantie optreden. Het is perfect denkbaar dat een systeem zoals dat van Cambridge Analytica volledig geautomatiseerd gebeurt, maar dat zou het probleem niet wegnemen. Ook geautomatiseerde systemen kunnen tot dominantie leiden.

Dat blijkt uit onderzoek van big data experts, zoals dat van de wiskundige Cathy O'Neil naar destructieve algoritmes die ze '*weapons of math destruction*' (kortweg WMD) noemt.[10] Het grote probleem met WMD's is dat ze niet transparant zijn voor wie eraan onderworpen wordt en bijgevolg de macht die WMD's over hem/haar uitoefenen niet ter verantwoording kan roepen. Een voorbeeld dat ze geeft is dat van '*added-value modeling*' in de Amerikaanse stad Washington D.C. De stad wilde haar onderwijssysteem verbeteren en huurde een databedrijf in om een systeem te bedenken om de slechte leerkrachten uit de scholen te filteren. Leerkrachten kregen op basis van de verwerking van data door een algoritme een score. Scoorden de leerkrachten onder een bepaalde waarde, dan werden ze automatisch ontslagen. Leerkrachten die geëvalueerd werden door het systeem wisten niet hoe de score bepaald werd en kregen ook geen verdere uitleg bij ontslag. Het systeem bleek ook leerkrachten te elimineren die door directie, collega's, ouders en leerlingen als goed werden bevonden. De beleidsmakers waren echter van mening dat een algoritme objectiever was dan de evaluatie van mensen.

Uiteindelijk bleek achteraf dat veel leerkrachten, die vermoedden dat de resultaten een rol speelden in hun score, mogelijks met de examenresultaten van hun leerlingen geknoeid hadden. Testte een eerlijke leerkracht de leerlingen het jaar daarop opnieuw, dan leek het of de klas achteruitgegaan was in vergelijking met vorig jaar. Daardoor werden sommige goede leerkrachten mogelijks ontslagen omdat ze een klas voor zich kregen die eigenlijk zwakker was dan de vervalste examenresultaten lieten uitschijnen. De beleidsmakers erkenden dat er in sommige gevallen mogelijks geknoeid was, maar ze hielden vol dat het systeem over het algemeen goed werkte en dat het bewijs van mogelijke vervalsing niet afdoende was, en dat elke ontslagen leerkracht eerlijk behandeld was geweest.

O'Neil geeft ons nog tal van dergelijke voorbeelden. WMD's worden in de VS tegenwoordig gebruikt in het bepalen van een strafmaat, bij ordehandhaving en bij het toekennen van jobs of leningen via bijvoorbeeld een credit-score systeem. Zelfs een goed werkend systeem zal fouten maken. Bovendien genereren deze systemen een score die iets zegt over de *waarschijnlijkheid* dat mensen slechte leerkrachten, recidivisten, slechte werknemers of mogelijke criminelen zijn. Mensen krijgen niet de kans om tegen de score die hen toegekend wordt te argumenteren. In het algemeen weten ze zelfs niet hoe die score tot stand komt. O'Neil merkt dan ook terecht op dat WMD's efficiëntie prefereren boven rechtvaardigheid en dat ze vaak het verleden van mensen projecteren in de toekomst waardoor ze ook tot *self-fulfilling prophecies* leiden.

Het probleem is niet dat anderen over je schouder kunnen meekijken. Het probleem is de creatie van een niet-contesteerbare en willekeurige macht.

Bovenstaande voorbeelden tonen het gevaar van het blinde vertrouwen op big-datatechnologie. Zelfs al deze data volledig anoniem en zonder verder menselijke tussenkomst verwerkt worden, zijn dergelijke systemen verwerpelijk. Dat anderen over je schouder kunnen meekijken, is niet het probleem. Het probleem is de creatie van een niet-contesteerbare en willekeurige macht. Of die macht een individu is dat over je schouder meekijkt om zo je gedrag te manipuleren of een niet-transparant algoritme dat een score uitspuwt en bepaalt welke mensen geviseerd worden als criminelen, of toegang hebben tot bepaalde jobs of leningen, maakt niet zoveel uit.

Naar een democratisering van de privacy-bescherming

Wat is de implicatie van deze visie op privacy voor het gebruik van datatechnologie in de strijd tegen corona? Ten eerste: anonieme dataverwerking is geen vol-

doende voorwaarde om dominantie tegen te gaan. Ten tweede: de macht die dergelijke technologie met zich meebrengt moet onder de controle vallen van zij die eraan onderhevig zijn. Op die manier voorkomen we dat deze macht willekeurig wordt.

Hier schuilt een groot gevaar, want zoals critici van de maatregelen opmerken, worden veiligheidsmaatregelen die in tijden van crisis genomen worden later zelden teruggeschroefd. Denk bijvoorbeeld aan de Amerikaanse PATRIOT-Act. De wet werd ingevoerd in 2001 na de aanslagen op 11 september van datzelfde jaar. De wet gaf veiligheidsdiensten meer bewegingsruimte en liet het onder meer toe om massaal telefoongesprekken af te luisteren. Nadat de wet gedeeltelijk werd teruggedraaid in 2015, onder de naam 'Freedom-Act', is ze voor een groot deel nog steeds van kracht.

Combineer de weerbarstigheid van dergelijke maatregelen met O'Neil haar stelling dat WMD's vaak van het ene domein naar het andere overspringen en het is niet ondenkbaar dat toekomstige regeringen (ongetwijfeld met de beste bedoelingen) het systeem van *track & trace* zullen behouden en uitbreiden of heroriënteren voor misdaad of terreurbestrijding. Zeker omdat nog niet meteen een vaccin in zicht is en de dreiging van nieuwe pandemieën altijd om de hoek blijft loeren, is de kans reëel dat deze maatregelen het nieuwe normaal worden en we geleidelijk aan slaapwandelen in de proliferatie ervan. Waakzaamheid is dus zeker geboden om te garanderen dat de maatregelen in tijd en omvang beperkt blijven.

Om te voorkomen dat de macht die de implementatie van deze technologie met zich meebrengt geen willekeurige macht wordt, kan het gebruik van dergelijke maatregelen alleen maar als er een grote democratische controle over is. Toegegeven, in België zitten we op dit vlak beter dan veel andere landen. Zo houdt de Gegevensbeschermingsautoriteit, opgericht naar aanleiding van de fameuze Europese GDPR-wet, toezicht op de 'Data against corona'-taskforce.

Maar vanuit het gezichtspunt dat ik hier hanteer, is dat onvoldoende. Overweging 16 van de GDPR stelt immers onomwonden dat de regelgeving niet van toepassing is op (onder meer) zaken van nationale veiligheid. In deze context zijn de besluiten van de Gegevensbeschermingsautoriteit niet absoluut afdwingbaar ten opzichte van de overheid. We moeten er ook rekening mee houden dat onze huidige regering een regering met 'bijzondere machten' is, die de overheid vrij verregaande volmachten geeft om de coronacrisis op te lossen, ook met betrekking tot openbare orde en volksgezondheid. Er moeten dus absolute garanties zijn dat we de burgerlijke controle over de maatregelen vrijwaren en dat deze burgerlijke controle het laatste woord heeft (wat op dit moment niet het geval is).

Het gebruik van dergelijke technologie kan dus alleen maar wanneer de macht die ze het in het leven roept contesteerbaar blijft en onder de controle van de burger blijft. Om dit te realiseren stel ik volgende algemene maatregelen voor die van kracht dienen te zijn voor eender welk gebruik van big data technologie door de overheid – dus niet alleen in deze crisis:

1. De gebruikte software en modellen moeten volledig openbaar zijn, vergezeld van toegankelijke informatie die de werking ervan toelicht. Op die manier kan elke burger zien hoe de macht in elkaar zit, of ze redelijk is en kan de burger deze macht contesteren.

2. Er moet een wettelijk kader van kracht zijn dat de Gegevensbeschermingsautoriteit een vetomacht geeft over de implementering van eender welke maatregel, ook in gevallen van nationale veiligheid, en die ook garandeert dat de Gegevensbeschermingsautoriteit op eender welk moment een maatregel kan herroepen.

3. De Gegevensbeschermingsautoriteit moet gedemocratiseerd worden door toevoeging van een burgerpanel. Ook al is de Gegevensbeschermingsautoriteit een onafhankelijk orgaan, het blijft bestuurd door een select clubje van bureaucraten en specialisten die mee aan de knoppen van de macht zitten en keuzes voor ons maken. De expertise van deze specialisten is cruciaal, maar onvoldoende. We kunnen van deze crisis gebruikmaken om de macht verder te democratiseren, door een burgerpanel op te richten, met leden bepaald door lottrekking en bijgestaan door de experten van de Gegevensbeschermingsautoriteit. De experten adviseren de burgers, maar uiteindelijk is het aan de burgers zelf om de beslissing te maken.

Een vrije samenleving is alleen mogelijk als burgers zelf controle over deze macht hebben, en geen select clubje van bureaucraten, advocaten, computerwetenschappers, filosofen of epidemiologen.

Eindnoten

1 Cf. bijv. T. Van de Weghe & R. Van Den Heuvel (2020), 'Is technologie onze exit-strategie uit de coronacrisis?' VRT NWS.

2 M. Dobbelaere-Welvaert (2020), 'De wereld staat in brand. Willen we na corona wakker worden in een wereld met of zonder privacy?' Knack.be.

3 Y. Harari (2020), 'Alles wordt totaal anders.' *De Morgen*.

4 M. Boudry (2020), Tweet 22 maart 2020.

5 M. Boudry (2014), 'Privacy-hysterie.' *De Standaard*.

6 P. Haeck & P. Depuydt (2020), 'Apps tegen corona: Opgelet, u kwam in contact met een coronapatiënt.' *De Tijd*.

7 Knack/Belga (2019), 'Google-medewerkers luisteren mee naar uw gesprekken, ook in uw huiskamer.' Knack.be.

8 P. Pettit (1999), *Republicanism: A Theory of Freedom and Government.* Oxford University Press.

9 P. Huyghebaert / Belga (2018), 'Groot Facebooklek: bedrijf van Bannon maakte gegevens van 50 miljoen mensen buit.' VRT NWS.

10 C. O'Neil (2016), *Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy.* Crown Random House.

Louis Mosar is filosoof en lid van Denktank Minerva.

louis.mosar@gmail.com

Denktank Minerva is een onafhankelijke denktank binnen de brede progressieve beweging. Met scherpe opinies en sterke, onderbouwde studies wil Minerva de progressieve stem doen weerklinken in het maatschappelijke debat. Denktank Minerva houdt bestaande denkwijzen tegen het licht, en toont dat er concrete, haalbare, en wenselijke alternatieven zijn.

www.denktankminerva.be
info@denktankminerva.be
@DenktankMinerva