

Making Surveillance Public: Why You Should Be More Woke About AI and Algorithms

SOFIE ROYER^a

Schuilenburg, M. (2024). *Making Surveillance Public. Why You Should Be More Woke About AI and Algorithms*. Eleven.



Panopticon, 46 (1), 87-89

© 2025 Maklu | ISSN 0771-1409 | Januari 2025

^a Onderzoeksexpert CiTiP KU Leuven, gastprofessor ULiège (corresp.: sofie.royer@kuleuven.be)

Wat is de gelijkenis tussen het panopticon en een Tesla? Het antwoord op die vraag, die klinkt als het begin van een (slechte) mop, is dat het allebei manieren zijn om surveillance te organiseren. Althans, dat vindt de Nederlandse criminoloog en filosoof Marc Schuilenburg in zijn meest recente boek, *Making Surveillance Public*. Het model voor stervormige gevangenissen van Jeremy Bentham behoeft wellicht weinig uitleg voor de lezers van dit tijdschrift. De Tesla is een wagen die uitgerust is met een systeem dat verdachte bewegingen in de omgeving van het voertuig met een viertal camera's monitort, en aan de eigenaar signaleert en zo vandalisme en diefstal moet voorkomen.

Net zoals Tesla's zijn ook slimme deurbelcamera's en de navigatieapplicatie Waze volgens Schuilenburg voorbeelden van *luxury surveillance*. Met een Ring Video-deurbel van Amazon kan je niet alleen vanop afstand controleren wie er voor de deur staat; de beelden kunnen ook met de politie worden gedeeld. En wie de weg zoekt, kan met de navigatieapp Waze een traject kiezen dat (waarschijnlijke) hotspots van criminaliteit vermijdt. In tegenstelling tot het panopticon, waarin gedetineerden externe surveillance verplicht moeten ondergaan, zijn dit voorbeelden van vormen van surveillance waarvoor mensen vrijwillig overstag gaan en soms (veel) geld neertellen. *Luxury surveillance* gaat gepaard met de verzameling van grote hoeveelheden persoonsgegevens, die door algoritmen worden gestuurd met het oog op of onder het mom van een veiligere samenleving.

Met zijn boek over algoritmische surveillance wil Schuilenburg het bewustzijn over de inzet van artificiële intelligentie en algoritmes in de samenleving vergroten. Hij gaat na wat de maatschappelijke impact is van algoritmes die met het oog op meer veiligheid door publieke én private spelers worden ingezet. De auteur onderzoekt of er positieve gevolgen zijn voor de samenleving. Kunnen algoritmes ervoor zorgen dat er minder criminaliteit is? Daarnaast formuleert hij ethische bedenkingen. Is het wenselijk dat Amazon 24/7 weet wat er in de omgeving van je huis gebeurt? Leiden navigatieapps die bepaalde buurten ontwijken tot een nieuwe vorm van segregatie? Hoe vrij kunnen mensen nog zijn in de publieke ruimte als algoritmes permanent hun gedrag bijsturen? Schuilenburg vult zo, naar eigen zeggen, een lacune in het criminologische onderzoek, waar surveillance altijd al een onderbelicht thema was.

Na een introductie over het bestaande onderzoek naar surveillance in een notendop, snijdt de auteur het algemene thema aan in vier hoofdstukken en vier intermezzo's. Hij begint met de vraag waarom burgers hun gegevens vrijwillig aan privébedrijven toevertrouwen. Voorts gaat hij in op de centrale plaats van surveillance in onze samenleving. In het bijzonder heeft hij oog voor de nieuwe machtsrelaties die ontstaan door technologische innovatie, wat hij *algorithmic psychopower* noemt. *Big data policing* is het volgende onderwerp. Met een intermezzo van boeken, films en series over digitale surveillance kan de lezer zijn kijk- en leeslijst aanvullen. Vervolgens stelt Schuilenburg zich de vraag hoe algoritmes beheersbaar en controleerbaar kunnen blijven. Dan volgt een pleidooi voor meer aandacht voor de menselijke beleving van algoritmes. De auteur rondt zijn betoog af met een agenda voor criminologisch onderzoek naar de rol van algoritmes in het veiligheidsbeleid. Het boek bevat tot slot een hoofdstuk met prentjes die passen bij de aangesneden onderwerpen.

Schuilenburg heeft een bijzonder actueel en noodzakelijk onderwerp te pakken en dat maakt van het boek een aanrader. Algoritmes sluipen onze samenleving binnen zonder dat we er erg in hebben. Tegelijkertijd klinkt de roep naar een strenger veiligheidsbeleid steeds luider. Ook in onze contreien lokken voorstellen om technologische innovaties in te zetten om een veiligere samenleving af te dwingen, weinig tot geen kritische reacties uit.¹ Wat dat betreft is het boek een welgekomen aanzet om het tot nog toe quasi onbestaande maatschappelijke debat over de wenselijkheid van die surveillancetechnologieën te voeren. Het boek is overigens doorspekt met sprekende voorbeelden die de lezer met de neus op de feiten drukken. Zo maken sommige voetbalstadions in Nederland blijkbaar niet alleen beelden van supporters, maar ook individuele geluidsopnames om negatieve emoties, zoals racistische uitlatingen, te detecteren en te beïnvloeden. Zogenaamde slimme toiletten zouden een enorm potentieel voor gezondheidsmonitoring hebben en zelfs toiletbezoekers herkennen aan hun 'anusafdruk'. Het hoeft niet te verbazen dat autofabrikanten heel wat – lees: meer dan nodig – gegevens verzamelen, zoals de gewenste temperatuur in de wagen en de favoriete bestemmingen van de bestuurder. Maar dat ze via het unieke profiel ook inzicht kunnen krijgen in het seksleven van de bestuurder, is best griezelig. Het panopticon van vandaag is met andere woorden een rondrijdende *panopticar*.

Wel is het niet helemaal duidelijk wie het doelpubliek is van het boek. De omvang en uitgave doen vermoeden dat het boek als wetenschapscommunicatie bedoeld is. Als lezer moet je niettemin over een gedegen voorkennis beschikken om je een weg door het boek te banen, onder meer door de vele niet-alledaagse concepten die in ijltempo de revue passeren, zoals *system technology*, *algocracy*, *synoptic surveillance*, *surveillance feudalism* ... Door de afwisseling tussen hoofdstukken en intermezzo's is de rode draad van het verhaal soms moeilijk te volgen. Enkele inhoudelijke uitgangspunten zijn bovendien voor kritiek vatbaar. Zo lijkt Schuilenburg er in het eerste intermezzo '*Data Donation*' van uit te gaan dat burgers hun gegevens vrijwillig delen met bedrijven, terwijl er heel wat privacy-moeite heerst. Dat leidt ertoe dat burgers net minder moeite doen om hun online privacy te beschermen.² Het is tot

- 1 Bijvoorbeeld het voorstel om gezichtsherkenningcamera's in te zetten om sluikstorters te identificeren (fem, "Conner Rousseau: "Laten we camera's met gezichtsherkenning uitproberen tegen sluikstorters"", *Het Nieuwsblad* 4 oktober 2024, https://www.nieuwsblad.be/cnt/dmf20241004_94496132) of de inzet van drones om fietsstraten af te dwingen (A. Goegebeur, "Politie zet drones in om bestuurders te controleren: "Is veiligheid van fietsers minder belangrijk dan privacy?"", maandag 23 september 2024, https://www.standaard.be/cnt/dmf20240923_93855484).
- 2 Hanbyul Choi, Jonghwa Park, Yoonhyuk Jung, "The role of privacy fatigue in online privacy behavior", *Computers in Human Behavior* 2018, p. 42-51.

slot jammer dat de auteur achterhaalde terminologie gebruikt, zoals kinderpornografie,³ terwijl hij er zelf op wijst dat woordkeuze een belangrijke rol speelt in de perceptie van fenomenen. Zo dragen schattige begrippen als *cookies* en *the cloud* bij tot een maatschappelijk klimaat waarin surveillance meer acceptabel voorkomt.

Schuilenburg is professor digitale surveillance aan de Erasmus University Rotterdam. Het boek vloeit voort uit zijn oratie getiteld *'Making Surveillance Public: Waarom we in gesprek moeten over big data en algoritmes als het over veiligheid gaat'* (23 juni 2023). Het boek leest dus ook als een onderzoeksagenda met een overzicht van thema's waarop zijn onderzoeksgroep de komende jaren zal focussen. Dat verklaart enerzijds waarom zoveel verschillende problematieken slechts vluchtig worden aangestipt en anderzijds waarom het boek, hoewel het nooit echt (te) technisch wordt, wel academisch en niet altijd toegankelijk is geschreven. Lezers met voorkennis over of interesse in de rol van technologie in de samenleving, zullen het boek zeker weten te appreciëren. De vraag is echter of het boek ook een ruimer doelpubliek kan bereiken, wat nodig is om het maatschappelijke debat over de algoritmes en veiligheid écht op gang te brengen.

3 <https://www.interpol.int/Crimes/Crimes-against-children/Appropriate-terminology>.