Oratie: Waarom we in gesprek moeten over big data en algoritmes als het over veiligheid gaat.

Marc Schuilenburg (Erasmus Universiteit Rotterdam en Vrije Universiteit Amsterdam)

Jurist en filosoof Marc Schuilenburg is benoemd tot bijzonder hoogleraar Digital Surveillance aan de Erasmus Universiteit. Op vrijdag 23 januari vindt de oratie plaats van getiteld "Making Surveillance Public: Waarom we in gesprek moeten over big data en algoritmes als het over veiligheid gaat". In de nieuwsbrief licht hij al een tipje van de sluier op.

Het veiligheidsvraagstuk verandert door de maatschappelijke trend van digitalisering en het gebruik van big data en algoritmes door publieke en private partijen in het bijzonder. De politie, rechtspraak en het gevangeniswezen omarmen steeds meer big data-achtige instrumenten en deze toepassingen hebben consequenties voor het politiewerk en in een breder verband ook voor de strafrechtspleging en -toepassing. Aan dit rijtje van partijen kunnen buitenlandse bedrijven zoals Amazon, Google en Tesla worden toegevoegd. Deze techbedrijven worden in toenemende mate een machtsfactor van betekenis in het Nederlandse veiligheidsvraagstuk en vullen een existentiële veiligheidsbehoefte op van groepen burgers. Hoe verandert het gebruik van big data en algoritmes de aanpak van criminaliteit en overlast? Maar ook: hoe kunnen ethiek en de rechtsstaat deze nieuwe technieken beheersbaar en controleerbaar houden? Dat zijn kwesties die meer aandacht verdienen in de criminologie, zo stel ik in mijn oratie op 23 juni 2023 aan de Erasmus Universiteit Rotterdam – met de titel: 'Making Surveillance Public'.

In de wereld van nu is de omvang en de diepgang van digitale surveillance substantieel toegenomen, van het massaal verzamelen van data in domeinen zoals de rechtshandhaving tot het diep doordringen in het privéleven van burgers door private bedrijven met surveillancetechnieken die niet als zodanig meer worden herkend omdat zij een onderdeel zijn geworden van het dagelijkse leven, van slimme deurbellen tot thermostaten die zelf beslissingen nemen. Digitale surveillance organiseert en oriënteert de samenleving en iedereen participeert hieraan in meer of minder mate mee. Met betrekking tot big data en algoritmes in het politiewerk gaat de meeste aandacht hierbij uit naar het fenomeen van predictive policing. Maar de opkomst van luxe surveillance zoals de slimme Amazon deurbel Ring en de Sentry Mode-bewakingsmodus in de auto's van Tesla bewijst dat meer partijen zich bezighouden met het veilig maken van de samenleving en dat bovendien doen met hun eigen big data-achtige-tools. Tal van ongewenste neveneffecten kunnen hierbij optreden waaronder geautomatiseerd etnisch profileren en het zogeheten *black box*-scenario, waarmee wordt bedoeld dat algoritmische besluitvorming niet alleen voor buitenstaanders niet-toegankelijk en daarmee oncontroleerbaar is, maar ook door gebruikers zelf niet meer wordt begrepen of kan worden uitgelegd.

Een belangrijke vraag die in mijn oratie aan bod komt, is hoe vormen van digitale surveillance 'publiek' kunnen worden gemaakt. Veiligheid en efficiëntie zijn belangrijke publieke waarden, maar dat zijn het recht op gelijke behandeling en de privacy van burgers ook. Tussen beide kanten van 'publiek maken' schuilt onlosmakelijk een spanning en ik ben geïnteresseerd hoe in de ontwerp- en ontwikkelfase van nieuwe technologie, dus bij de eerste ontwikkeling ervan, al rekening kan worden gehouden met datgene wat we als samenleving belangrijke waarden vinden. Dit zou onder andere kunnen door andere personen als alleen ICT-experts te betrekken bij de ontwikkeling van nieuwe digitale toepassingen. Op die manier kan een stem worden gegeven aan iedereen wie dat op dit gebied nog niet of onvoldoende heeft, waaronder de 'silenced voices' van zwakke, kwetsbare of gemarginaliseerde groepen.

Opvallend is dat er nog nauwelijks stevige empirische onderzoeken zijn naar de effecten van big data-achtige toepassingen en de schaarse evaluaties die er wel zijn, laten vaak tegenstrijdige en wisselende resultaten zien. Zelden wordt onderzocht of een concrete toepassing werkt en of de werking in verhouding staat tot de opbrengst ervan. Het simpele feit dat iets mogelijk is, maakt het immers niet meteen wenselijk. Weegt het oogmerk van een big data-achtige toepassing bijvoorbeeld op tegen de meerwaarde van andere oplossingen in de aanpak van criminaliteit en overlast? Het is daarom van belang dat op dit gebied meer kennis wordt vergaard of toepassingen wel het effect sorteren dat wordt beoogd, en ook of er, ondanks alle goede bedoelingen, niet een tegengesteld effect wordt bereikt.

Met mijn benoeming als bijzonder hoogleraar Digital Surveillance wil ik met mijn promovendi onderzoek doen hoe het werkelijk zit met de effecten van big data-achtige toepassingen en de sociale interacties tussen het publiek en de veelheid aan partijen op dit gebied om zo het perspectief en de betekenissen die deze personen geven aan surveillance beter te leren kennen. Van oudsher staat de mens centraal in de criminologie, maar wanneer van 'actoren' wordt gesproken, dan zal criminologisch onderzoek zich ook moeten richten op alles wat 'niet-mens' is, waaronder de *agency*, het handelend vermogen, van algoritmes in de veiligheidspraktijk. Technische kennis kan meer inzicht geven in het nut dan wel de risico's van big data en algoritmes. Maar ik denk ook aan criminologische onderzoeksmethoden die andere vormen van kennis opleveren, waaronder participerende observaties vanuit de etnografische traditie en een narratief criminologisch perspectief.

Mijn oratie over het publiek maken van digitale surveillance is uiteindelijk een pleidooi voor een digitale criminologie, waarin het gaat om hoe de 'digital turn' het speelveld van de criminologie verandert. In termen van de aard, omvang en achtergronden van cybercriminaliteit natuurlijk, maar het blijft hiertoe niet beperkt. Een digitale criminologie richt zich ook op wat digitalisering teweegbrengt – direct of indirect – op gebieden van ordehandhaving, strafrechtspleging en veiligheidsbeleid: welke digitale tools en door wie ze worden gebruikt, tot welke resultaten ze leiden, en, niet minder belangrijk, tegen wie ze worden gebruikt.