Bijdrage Vives-lector(en) Onderzoek AI tekstvereenvoudiging

Eigen aanpassingen

[schrijf hier extra aanpassingen die niet op pagina 2 van de richtlijnen staan, indien aangebracht]

Tekst van het vereenvoudigde artikel

Inleiding

Vandaag de dag gebruikt de politie artificiële intelligentie (AI) en 'big data', deze manier van werken noemt men ook wel algoritmische surveillance. Hierbij maakt men gebruik van algoritmische systemen die

1. gebruik maken van op regels gebaseerde algoritmen om gestructureerde en ongestructureerde gegevens te classificeren, op te slaan, te combineren en te doorzoeken, om vastgelegde gegevens te vergelijken met andere gegevens en overeenkomsten te vinden;

en

2. gebruik maken van machine-lerende algoritmes om patronen en bruikbare kennis in big data sets trachten te voorspellen op basis van de patronen die in de vastgelegde gegevens zijn gevonden. (Van Brakel, 2021)

Ook al werden reeds heel wat stappen gezet om het toenemende gebruik van algoritmische surveillance in te passen in het juridische kader, toch roept dit de vraag op of dit voldoende is om alle burgers te beschermen. In dit artikel proberen we de klassieke controle en handhavingsmechanismen te herdenken, aan de hand van drie socio-technologische ontwikkelingen en door ernaar te kijken met een relationeel ethische bril, zodat deze minder onder druk komt te staan.

Socio-technische ontwikkeling

Door de opkomst van algoritmische surveillance kunnen we drie socio-technische ontwikkelingen benoemen:

1) 'Fragmentatie en privatisering van politiewerk': door besparingen in de publieke sector zien we een stijging in samenwerking met de private sector waardoor er een machtsverschuiving plaatsvindt in het politiewerk. De agenten zijn zeer afhankelijk van private technologiebedrijven, omdat we steeds vaker van platform policing spreken bij politiewerk. Hier gebruiken de agenten digitale platformen en opsporingstechnologieën die eigendom zijn van de technologiebedrijven.
2) 'Democratisering van surveillance': Tegenwoordig gebruikt men steeds vaker grootschalige surveillance (bijvoorbeeld op vliegveld) in plaats van gerichte surveillance (volgen van een verdachte), dit wilt zeggen dat een veel groter deel van de bevolking onder toezicht staat. Dit zorgt dat de diensten en private bedrijven veel meer data hebben over de bevolking, bijvoorbeeld via de 'Pegasus-spyware' die data van smartphones kan verzamelen. Dit brengt dan weer een risico op machtsmisbruik met zich mee.
3) 'Toename van collectieve schade en sociale gevolgen': Doordat de analyse van big data gebeurd op basis van gegroepeerde kenmerken, wordt er op het eerste zicht geen persoonsgegevens verwerkt. Hierdoor krijg je een verdeling met

sociale lagen, dit met een ongelijke verdeling tussen maatschappelijke groepen. Vooral kwetsbare minderheidsgroepen zijn hier het slachtoffer van. Zij zijn vaker het doelwit van deze technologieën, die onterecht bepaalde vooroordelen bevestigen.

Het algoritme kan over bepaalde buurten afwijkende data krijgen, waardoor er een verkeerd negatief beeld wordt gevormd over deze buurten. Hierdoor wordt er meer politie gestuurd naar deze buurt (*predictive policing*), wat terug negatieve data over de buurt oplevert (uit feedback loops) Dit leidt dan weer tot meer politieaanwezigheid (*overpolicing*). Het gebruik van big data-analyses brengt dus het risico van discriminatie en stigmatisatie met zich mee, hieruit komen sociale gevolgen voort zoals het criminaliseren van (kans)armoede en een toename in de ongelijkheid in de samenleving.

Juridisch kader

Het huidig juridisch kader heeft in België heel wat tekortkomingen, baseert zich op de regels aangaande de gegevensbescherming en legt hierbij de focus op de informatieveiligheid (*Data Protection Impact Assessments* of DPIA's) endus niet op de bescherming van de fundamentele rechten. Daarnaast worden de burgers ook niet betrokken want de politie is niet verplicht om de DPIA's te publiceren, weinig transparant dus voor publieke controle. Wat de DPIA's betreft zijn er ook geen standaarden waar men zich aan moet houden en bestaat er geen standaardprofiel voor de functionaris die zich met gegevensbescherming bezighouden.

Ondertussen heeft de EU een AI-wet voorgesteld voor alle lidstaten, die zou moeten zorgen voor betere bescherming van het individu voor nadelige gevolgen van AI. Dit voorstel kan enkele van onze problemen rond controle- en handhavingsmechanismen opvangen, zoals de verplichting voor de lidstaat om minstens één nationale bevoegde autoriteit aan te wijzen die toezicht houdt over toepassingen van AI plus een officieel contactpunt voor de burger. De EU zal ook een databank opstarten waar toepassingen met een hoog risico in worden opgenomen, eenmaal op deze lijst zal het moeilijker op de Europese markt raken. Toch is het nog niet duidelijk hoe een toepassing beoordeeld zal worden en wat als standaard zal aangenomen worden, ook wordt de bevolking nog steeds niet betrokken en zouden ze geen klachten kunnen indienen bij de bevoegde nationale autoriteit.

Herdenken van algoritmische surveillance-controle

De Ubuntufilosofie vraagt een fundamentele verschuiving in het denken rond algoritmische onrechtvaardigheden, dit van rationele ethiek naar relationele ethiek. Dit houdt in dat we de schade en onrechtvaardigheden die door algoritmen worden veroorzaakt, niet los kunnen zien van de technologische-, sociale, economische en sociale context. Als we deze relationele visie toepassen op justitie en politie zou deze hervormt worden tot de bescherming van de collectieve

veiligheid, dit gaat verder dan de huidige visie (tegen criminaliteit). Er moet meer aandacht besteed worden aan andere oorzaken van onveiligheid: zoals bijvoorbeeld gezondheidszorg, onderwijs en werk, discriminatie,... Deze sociale en economische rechten worden vaak niet opgenomen in ons veiligheidsbeleid.

Relationele controle impliceert het betrekken van de belangen van de meest kwetsbare groepen en hun vertegenwoordigers in het beleid, maar ook in controlemechanismen die de sociaal-technische algoritmische surveillance als uitgangspunt neemt. Als laatste is ook transparantie een cruciaal onderdeel om te vermijden dat mensenrechten geschonden worden en het bevorderen van hun bescherming.

Concrete stappen

Er moet nagedacht worden over hoe controlemechanismen herdacht kunnen worden om de kwetsbaren en hun vertegenwoordigers te beschermen. De burgers moeten meer inspraak krijgen aan de hand van toetsen, in deze toetsen heeft men ook aandacht voor de verschuiving van macht naar de private sector. Zeker wanneer het gaat over grootschalige surveillance door politiediensten moet de bevolking betrokken worden om hun legitimiteit te bewaren. Dit weer vanuit de relationele ethiek om de kwetsbare groepen en gemeenschappen een stem te geven in de beslissingsprocessen.

Daarnaast kan men ook denken aan een AI-coördinatiecentrum dat aan het beleid, toezichthouders en uitvoerende organisaties een structuur biedt om regelmatig met elkaar af te stemmen rond verschillende kwesties. Zowel de toetsen als de structuur die het centrum aanbiedt moet worden gebaseerd op wetenschappelijk onderzoek gedaan door universiteiten.

Conclusies

Uit het artikel is gebleken dat het huidige kader voorlopig niet volstaat om druk van de socio-technische ontwikkelingen op te vangen die algoritmische surveillance met zich meebrengen. Ook wanneer we kijken om het huidige kader te gaan herdenken rond controle en handhaving aan de hand van ‘rationele’ controlemechanismen wordt dit probleem niet opgelost. Toch biedt het ‘rationele’ kader interessante mogelijkheden om mee verder te werken.

Bibiografie

Van Brakel, R. 2021. *“How to Watch the Watchers? Democratic Oversight of Algorithmic Police Surveillance in Belgium”*. Surveillance & Society 2021, 19(2), 228-240.