De controle op het gebruik van algoritmische surveillance onder druk? Een exploratie door de lens van de relationele ethiek

Sinds het einde van de 20ste eeuw zijn er als gevolg van technologische ontwikkelingen nieuwe mogelijkheden ontstaan om data te verzamelen en te analyseren. De opkomst van 'big data' en de toegenomen mogelijkheden van artificiële intelligentie (AI) in de 21ste eeuw zijn met veel interesse omarmd door de politie. Het gebruik van deze technologieën door de politie kan worden beschreven als algoritmische surveillance. Dit zijn 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.[2]

Ondanks de toegenomen regelgeving[3], die als doel heeft de democratische waarborgen te garanderen van algoritmische surveillance, lijkt dit het gebruik ervan eerder te stimuleren.[4] Denk bijvoorbeeld aan de significante toename van het gebruik van 'intelligent' cameratoezicht in België, maar ook elders in Europa.[5] Dit roept de vraag op of de huidige controlemechanismen voldoende zijn om alle burgers te beschermen tegen de mogelijke gevolgen van het gebruik van algoritmische surveillance door de politie. Het doel van deze bijdrage is om na te denken over de vraag of huidige controle en handhavingsmechanismen voor het gebruik van algoritmische surveillance door de politie herdacht zouden moeten worden. Om tot een (voorlopig) antwoord op die vraag te komen zal ik in het eerste deel van het artikel drie socio-technische ontwikkelingen bespreken die het huidig kader onder druk zetten. In het tweede deel zal ik huidige controleren handhavingsmechanismen bekijken door de bril van de relationele ethiek om te exploreren hoe we hieruit kunnen leren om controlemechanismen te herdenken.

Controle- en handhavingsmechanismen onder druk: socio-technische ontwikkelingen

Als gevolg van de opkomst van algoritmische surveillance in het politiewerk kunnen drie sociotechnische ontwikkelingen geïdentificeerd worden die het traditionele controle- en handhavingskader onder druk zetten: 1) de fragmentatie en privatisering van politiewerk, 2) de democratisering van surveillance, en 3) de toename van collectieve schade en sociale gevolgen. Deze ontwikkelingen zijn overlappend en verstrengeld en moeten niet als losstaande ontwikkelingen worden gezien. Ten eerste, fragmentatie en privatisering van politiewerk is niet nieuw. Sinds het einde van 20ste eeuw is er in het Westen een stijging van de samenwerking met de private sector en spelen private spelers een steeds grotere rol in politiewerk. Dit is in belangrijke mate het gevolg van de toegenomen macht en groei van de private sector en bezuinigingen in de publieke sector.[6] De technologische ontwikkelingen van big data en AI in het begin van de 21ste eeuw hebben geleid tot de toenemende macht van technologiebedrijven door onder meer 'surveillance kapitalisme', waarbij gegevensverzameling een economische drijfveer wordt voor bedrijven.[7]

Politiewerk wordt in toenemende mate *platform policing*, waarbij de politie gebruikt maakt van digitale platformen en digitale opsporingstechnologie.[8] Dit heeft als gevolg dat de politie steeds afhankelijker wordt van infrastructuur van technologiebedrijven[9] en leidt tot verschuivende machtsverhoudingen van de publieke naar de private sector, wat een negatieve invloed heeft op transparantie en controle.[10] Ten tweede, kan er een 'democratisering' van surveillance worden herkend door een verschuiving van aandacht voor gerichte surveillance naar grootschalige surveillance.[11] Hierdoor staat nu een veel groter deel van de bevolking onder surveillance waardoor het risico op toename van de macht van de staat maar ook van private actoren steeds groter wordt. Waarbij grootschalige surveillancepraktijken vroeger vooral werden uitgevoerd door intelligentiediensten[12] of binnen een bepaalde context zoals op het vliegveld, spelen politiediensten maar ook technologiebedrijven hierin een steeds grotere rol. Denk bijvoorbeeld in België aan de significante uitbreiding

van het gebruik van 'intelligent' cameratoezicht voor allerlei doeleinden[13], wat nog meer werd aangewakkerd door de coronapandemie.[14] Andere voorbeelden zijn de infiltratie van het versleutelde Encrochat-netwerk[15], de gezichtsherkenningssoftware van Clearview AI dat ook uitgeprobeerd is door de federale politie in België[16], of de dataverzamelingspraktijken van Europol[17] die door sommige vergeleken worden met surveillance praktijken van de Amerikaanse NSA.[18] Denk ten slotte aan het gebruik van de spionagesoftware Pegasus om data te verzamelen van mobiele telefoons van activisten, politici en journalisten over de hele wereld.[19] Ten derde is er steeds meer sprake van collectieve en sociale schade naast individuele schade. Een belangrijk kenmerk van big data-analyses is dat ze op geaggregeerd niveau plaatsvinden. Er worden dus op het eerste gezicht geen persoonsgegevens verwerkt.[20] Een van de gevolgen is een toename van sociale stratificatie, met een ongelijke verhouding tussen maatschappelijke groepen als gevolg.

Doordat big data onregelmatigheden en afwijkingen in datasets reproduceert kan dit leiden tot uitkomsten die een onevenredige impact hebben voor bepaalde groepen of gemeenschappen. Dit kan dan tot een cumulatief nadeel (discriminatie en oneerlijke behandeling) leiden voor bepaalde groepen in de maatschappij, omdat deze, vaak kwetsbare, groepen bovengemiddeld het doelwit zijn van deze technologieën.[21] Dit komt bijvoorbeeld duidelijk tot uiting bij *predictive policing*. Als gevolg van *feedback loops*, die ontstaan door steekproefbias, wordt politie herhaaldelijk teruggestuurd naar dezelfde wijken ongeacht het werkelijke misdaadcijfer.[22] Dit leidt tot *overpolicing* en stigmatisering van bepaalde al geviseerde wijken en gemeenschappen.[23] Deze risico's op discriminatie en stigmatisering door het gebruik van big data-analyses worden ook bevestigd in de uitspraak in Nederland over het gebruik van SyRI, een algoritmisch systeem om sociale fraude op te sporen. Daarnaast toont de uitspraak ook aan hoe big data-technologie sociale gevolgen heeft en naast discriminatie en stigmatisering ook bijdraagt tot het criminaliseren van armoede en kansarmoede en aan de toename van ongelijkheid in de samenleving.[24] Hierboven heb ik drie socio-technische ontwikkelingen beschreven die huidige controlemechanismen onder druk zetten. In het verdere verloop van deze bijdrage reflecteer ik over de vraag of huidige controlemechanismen om kunnen gaan met deze ontwikkelingen. Ik doe dit vanuit de lens van relationele ethiek.

Het huidige juridisch kader

Zoals deze bijdrage duidelijk maakt, zetten sociotechnische ontwikkelingen traditionele controle- en handhavingsmechanismen onder druk. De vraag stelt zich of het huidige juridisch kader voldoende is om met deze drie ontwikkelingen om te gaan en effectieve democratische waarborgen te voorzien. Het juridisch kader wordt vandaag gevormd door de regels aangaande de gegevensbescherming. De controle-instrumenten die daarbij momenteel ingezet worden voor de verwerking van gegevens door middel van AI, zoals toezichtsorganen, functionarissen voor gegevensbescherming en gegevensbeschermingseffectbeoordelingen (*Data Protection Impact Assessments* of DPIA's), zijn vaak beperkt in hun reikwijdte. De focus ligt grotendeels op informatieveiligheid en de formele naleving van het wettelijk kader. Er wordt daarentegen te weinig nadruk gelegd op de bescherming van fundamentele rechten, en meer specifiek vanuit artikel 8 van het EVRM.[25]

De manier waarop deze instrumenten werken in België is bovendien weinig democratisch, omdat burgers en het middenveld niet worden betrokken. Daarnaast is de politie niet verplicht DPIA's te publiceren volgens de politie en justitierichtlijn. Hierdoor wordt publieke controle bemoeilijkt. Er bestaan ook geen standaarden waaraan DPIA's moeten voldoen. Noch zijn er standaardprofielen voor functionarissen voor gegevensbescherming. Het huidige wettelijke kader betreft enkel toepassingen van algoritmische surveillance die 'persoonsgegevens' verzamelen en verwerken.[26] De EU publiceerde intussen een voorstel van AI-wet dat een tweevoudig doel heeft: de bescherming van de grondrechten van het individu tegen de nadelige gevolgen van AI, en daarnaast de harmonisatie van de regelgeving van lidstaten om mogelijke handelsbelemmeringen op de interne markt weg te nemen. De nadelige gevolgen van AI worden opgesplitst in risico-categorieën van laag naar hoog en er wordt in de verordening naast risico's voor het individu ook gesproken over risico's voor de samenleving. De verordening maakt echter niet duidelijk wat deze risico's juist zijn.[27]

Wat betreft controle- en handhavingsmechanismen is de voorgestelde verordening hoopvol. Het geeft aan dat lidstaten één of meer nationale bevoegde autoriteiten moeten aanwijzen om toezicht te houden op de toepassing en uitvoering van AI en als officieel contactpunt voor het publiek en andere actoren moeten fungeren. Ook wordt benadrukt dat de handhavingsmechanismen versterkt kunnen worden "door de invoering van een Europees coördinatiemechanisme dat in de passende capaciteit voorziet en audits van de AI-systemen vergemakkelijkt met nieuwe eisen inzake documentatie, traceerbaarheid en transparantie".[28] De verordening

geeft ook aan dat er een systeem zal opgezet worden om autonome AI-toepassingen met een hoog risico te registreren in een openbare databank voor de hele EU en dat deze enkel toegelaten zullen worden op de Europese markt indien zij voldoen aan “bepaalde dwingende voorschriften en vooraf een conformiteitsbeoordeling ondergaan.”[29] De manier waarop deze beoordelingen concreet in de praktijk toegepast en gehandhaafd zullen worden blijft echter vaag. Het is onduidelijk hoe de conformiteitsmechanismen eruit zullen zien. Ook schiet de verordening tekort op democratisch vlak, omdat burgers of het middenveld niet betrokken worden bij deze mechanismen. Bovendien zouden burgers ook geen klacht kunnen indienen bij de nationale toezichthoudende autoriteit, indien zij menen dat de wet niet wordt nageleefd.[30]

Herdenken van algoritmische surveillance-controle mechanismen door de lens van relationele ethiek.

Hieronder reflecteer ik over wat we kunnen leren uit de relationele ethiek, geïnspireerd door Ubuntufilosofie, om op een andere manier over controle in de algoritmische politiepraktijk na te denken, rekening houdend met de drie besproken socio-technische ontwikkelingen. Ubuntufilosofie heeft zijn oorsprong in Afrikaanse filosofie uit landen ten zuiden van de Sahara.[31] Ubuntufilosofie verschilt van traditionele rationele ethiek in de zin dat in tegenstelling tot rationele Kantiaanse ethiek, waarbij personen menselijke waardigheid hebben door hun vermogen tot autonomie, personen die menselijke waardigheid hebben omdat ze de capaciteit hebben om zich tot de andere te verhouden op een gezamenlijke manier.[32] Vanuit deze visie zijn mensenrechtenschendingen erop gericht om het vermogen van mensen tot gemeenschappelijke betrekkingen, opgevat als identiteit en solidariteit, ernstig te schaden; en moet menselijke waardigheid gezien worden als het menselijk vermogen om zich op een gemeenschappelijke manier tot anderen te verhouden.

Verschillende computerwetenschappers, die zich inspireren op Ubuntufilosofie, stellen een fundamentele verschuiving voor in het denken over algoritmische onrechtvaardigheid en bestuur van AI, van rationele ethiek naar relationele ethiek.[33] Volgens Birhane is relationele ethiek “een kader dat ons ertoe dwingt onze onderliggende werkhypothesen opnieuw te onderzoeken, ons ertoe dwingt hiërarchische machtsasymmetrieën te ondervragen, en ons ertoe aanzet de bredere, contingente en onderling verbonden achtergrond te beschouwen waar algoritmische systemen uit voortkomen (en worden ingezet) in het proces van bescherming van het welzijn van de meest kwetsbaren”.[34] Deze visie veronderstelt dat de schade en onrechtvaardigheid die door algoritmische systemen wordt toegebracht, niet los kan worden gezien van de filosofische beginselen van de technologie en de economische, politieke en sociale structuren die het mee vormgeven.[35]

Hoe kan deze visie verzoend worden met de visie van een politie- en justitie-apparaat dat vraagt naar steeds grootschaligere surveillance en samenwerken met de private sector?[36] Dit zou impliceren dat ook politiewerk vanuit dezelfde ethiek zou moeten vertrekken. Het zou betekenen dat de politieopdracht herdacht zou moeten worden op een relationele manier, als het beschermen van collectieve veiligheid. In het huidig beleid wordt veiligheid echter op een enge manier geïnterpreteerd als bescherming tegen criminaliteit en handhaving van de publieke orde. Vaak gaat het zelfs niet meer over veiligheid, maar om politieke drijfveren, om te laten zien dat er hard opgetreden wordt tegen criminaliteit. Het is een vorm van ‘surveillance theater’.[37] Vanuit een collectieve visie op veiligheid die als doel heeft om de veiligheid van alle burgers te vrijwaren, moet er meer aandacht besteed worden aan andere oorzaken van onveiligheid. Veiligheid is meer dan bescherming tegen criminaliteit alleen: gezond eten, proper water, huisvesting, basisinkomen, gezondheidszorg, onderwijs en werk, maar ook bijvoorbeeld niet het voorwerp zijn van discriminatie, pesterijen, haat, geweld en disproportionele controle van de overheid. Vaak worden deze sociale en economische rechten niet opgenomen in het veiligheidsbeleid.[38]

Wanneer men vanuit deze visie vertrekt, wordt het bijvoorbeeld duidelijk dat encryptie cruciaal is om mensenrechten en de meest kwetsbaren in de maatschappij te beschermen omdat door achterdeuren in te bouwen in de technologie, de veiligheid van bijvoorbeeld activisten en journalisten om democratische controle uit te oefenen wordt belemmerd.[39] Aangezien het zeker in het huidig politieke klimaat onwaarschijnlijk is dat veiligheid als sociale veiligheid gezien wordt, moet de vraag gesteld worden hoe de mazen van het net verfijnd zouden kunnen worden zodat controlemechanismen ervoor zorgen dat de meest kwetsbaren in de maatschappij beschermd worden.

Als we vanuit de relationele ethiek gaan kijken naar controle- en handhavingsmechanismen voor algoritmische surveillance dan impliceert dit dat het 'rationele' controle-kader, geconstrueerd vanuit het paradigma van gegevensbescherming, tekortschiet, zeker in de manier waarop dit in de praktijk en nationale politiewetgeving vertaald wordt. Het rationele kader gaat uit van mondige betrokkenen die individueel hun rechten kunnen beschermen door middel van informatieverzoeken, waarbij geen rekening wordt gehouden met kwetsbare groepen. Niet alle betrokkenen zijn gelijk. Ze hebben verschillende inzichten, niveaus van kennis, besluitvaardigheid, neiging om hun gegevens bekend te maken, en individuele kwetsbare eigenschappen. Factoren als leeftijd, geestelijk vermogen, kansarmoede, geletterdheid of geslacht kunnen van invloed zijn op het genot en de uitoefening van individuele rechten over gegevensbescherming.[40]

Controle moet daarom verder gaan dan enkel statische technische oplossingen en formele naleving van de wet, naar een praktijk die rekening houdt met de dynamische historische context en sociaal-technische praktijken waarin de technologie ingebed is, aandacht heeft voor machtsrelaties van de verschillende betrokken actoren, en waarin de bescherming van de meest kwetsbaren in de maatschappij voorop staat. Deze relationele controle impliceert het betrekken van de (belangen van) de meest kwetsbaren en hun vertegenwoordigers in het beleid alsook in controlemechanismen die het sociaal-technisch proces van algoritmische surveillance als uitgangspunt nemen.[41] Daarnaast is transparantie cruciaal om te vermijden dat vooroordelen en fouten leiden tot schendingen van de mensenrechten, zoals het Federaal Instituut voor de bescherming en bevordering van de rechten van de mens (FIRM) aangeeft. Volgens het FIRM weten mensen in België momenteel vaak niet voor welke beslissingen de overheid algoritmen gebruikt. Daarnaast is het ook niet altijd duidelijk hoe een algoritme persoonsgegevens verwerkt.[42]

Concrete stappen

Concreet houdt dit in dat er nagedacht moet worden over hoe controlemechanismen herdacht kunnen worden om met bovenstaande rekening te houden. Hoe kunnen ze rekening houden met asymmetrische machtsrelaties en de toenemende macht van technologiebedrijven? Hoe kunnen ze collectieve en sociale schade voorkomen? Vooraleer er besloten wordt om te investeren in (het ontwerpen van) een bepaalde technologie door de politie, moet er een democratische evidence-based proportionaliteitstoets uitgevoerd worden. Deze toets betrekt burgers bij de beslissingen. Bovendien heeft deze toets aandacht voor de toenemende macht van de staat en private partners alsook aandacht voor collectieve en sociale schade. Deze toets moet gebeuren op basis van wetenschappelijke en objectieve analyse. Hier zou bijvoorbeeld een orgaan zoals de Nederlandse onafhankelijke Raad voor Regeringsbeleid (WRR)[43] een rol kunnen spelen door beleidsgericht onderzoek te verrichten in nauwe samenwerking met universiteiten en het middenveld. Dit orgaan zou dan bijvoorbeeld ook onderzoek kunnen doen naar de collectieve en sociale schade van algoritmische surveillance en naar innovatieve controle en handhavingsmechanismen. Daarnaast zou men meer specifiek kunnen denken aan een AI-coördinatiecentrum, zoals het recente WRR AI rapport voorstelt, dat aan beleidsdirecties, toezichthouders en uitvoeringsorganisaties een structuur biedt om regelmatig en rond uiteenlopende kwesties met elkaar in contact te treden en van elkaar te leren. Dit centrum zou politiek verankerd moeten zijn, zodat er snel beleid kan worden gemaakt als dat nodig is.[44]

Zeker wanneer het gaat over grootschalige surveillance door politiediensten zou de bevolking betrokken moeten worden bij beslissingen om hun legitimiteit te bewaren.[45] Volgens het recente WRR-rapport over AI zal steeds vaker debat nodig zijn over de doelen die de samenleving wil nastreven en de vraag waar, waarvoor en onder welke condities de samenleving AI wil gebruiken. Methoden die hiervoor gebruikt kunnen worden, zijn bijvoorbeeld het organiseren van publieke debatten, openbare raadplegingen[46], burgerjury's, maar ook bijvoorbeeld de ondersteuning van citizen-science initiatieven.[47] Door het publiek te betrekken als actieve deelnemers aan het proces, kan de overheid leren van de expertise van burgers.[48]
Vanuit de relationele ethiek is het dan wel van essentieel belang dat kwetsbare groepen en gemeenschappen een significante stem krijgen in beslissingsmakingsprocessen en dat dit niet enkel 'voor de show' is. Samenvattend biedt relationele controle interessante pistes aan om huidige controlemechanismen te herdenken, op een manier die rekening houdt met de sociaal-technische ontwikkelingen beschreven in de aanvang van deze bijdrage.

Conclusie

In deze bijdrage heb ik gereflecteerd over de vraag of huidige controle- en handhavingsmechanismen

voor algoritmische surveillance herdacht zouden moeten worden. Eerst heb ik drie sociotechnische ontwikkelingen besproken die huidige controlemechanismen onder druk zetten. Nadien heb ik gekeken naar welke lessen we kunnen trekken als we controle- en handhavingsmechanismen voor algoritmische surveillance bekijken vanuit de relationele ethiek. Een voorlopig antwoord op de vraag is dat de drie socio-technische ontwikkelingen aangeven dat het huidig kader niet volstaat om deze ontwikkelingen op te vangen. Deze eerste exploratie van relationele ethiek om op een andere manier na te denken over controle en handhaving van gebruik van algoritmische surveillance door de politie, geeft aan dat 'rationele' controlemechanismen tekortschieten. Het relationele kader biedt interessante pistes om verder over de vooropgestelde vraag na te denken. Het antwoord in deze bijdrage blijft evenwel voorlopig, omdat verder (empirisch) onderzoek noodzakelijk zal zijn om hier beter inzicht in te krijgen.