

Een afwegingskader bij het invoeren van nieuwe technologie

VIER HANDVATTEN
VOOR BETROUWBARE
ALGORITMISCHE
TOEPASSINGEN
IN HET POLITIEWERK

Wereldwijd gebruiken politieorganisaties steeds vaker algoritmes om hun processen en taken te ondersteunen, met als doel om politiewerk beter en sneller uit te voeren. Deze algoritmische toepassingen lopen sterk uiteen en kunnen variëren in complexiteit, functies en toepassingen.

Er zijn applicaties die worden gebruikt om nieuwe vormen van criminaliteit te voorspellen. Andere toepassingen hebben als doel meer zicht te krijgen op actuele criminale fenomenen of op patronen die gerelateerd kunnen worden aan criminale gebeurtenissen in het verleden, bijvoorbeeld wapen- en drugs-handel op het dark web.

Technische mogelijkheden om data uit uiteenlopende bronnen te verzamelen en te analyseren via algoritmes hebben er mede aan bijgedragen dat de Nationale Politie steeds meer toepassingen op dit gebied zelf ontwikkelt. De politie hanteert hierbij verschillende instrumenten om over de inzet ervan een afgewogen oordeel te kunnen geven. Projecten waarin wordt gewerkt met grote hoeveelheden data worden getoetst aan de hand van het kwaliteitskader Big Data. Ook wordt een Gegevensbeschermings Effects Beoordeling (GEB of DPIA) opgesteld om nieuwe toepassingen

te kunnen toetsen. Met andere instrumenten wordt weer gekeken naar de ethische risico's om nieuwe technologie in te voeren.

De vier T's

Op dit moment bestaat er geen algemeen afwegingskader binnen de Nationale Politie om de bruikbaarheid van algoritmes en de maatschappelijke effecten hiervan te kunnen toetsen.¹ Ook bij politieorganisaties in andere landen doet dit probleem zich voor. Over het Britse politieapparaat spreekt de Justice and Home Affairs Committee in het rapport *Technology Rules?* van 'a new Wild West'.² Het is daarom tijd om te bewegen naar een uniform kader voor de ontwikkeling van algoritmische toepassingen in het politiewerk. Op basis van evidence-based literatuur over politieoptreden geven we in dit artikel hiervoor handvatten.³ We doen dit aan de hand van de vier 'T's': 1. *Targeted*; 2. *Tracked*; 3. *Talked* en 4. *Tested*.



Over de auteurs

Prof. mr. dr. Marc Schuilenburg is werkzaam aan de Erasmus Universiteit Rotterdam en de Vrije Universiteit Amsterdam. Drs. Martijn Wessels is werkzaam bij TNO en is promovendus aan de Erasmus Universiteit Rotterdam.



De afhankelijkheid van techniek kan ertoe leiden dat zaken als ‘intuïtie’ en ‘kennis van de buurt’ in het politiewerk verloren gaan

- 1 De minister van Justitie en Veiligheid op Kamervragen over het gebruik van algoritmes en surveillance door de Nationale Politie: <https://www.openkamer.org/kamervraag/2020Z17696/>.
- 2 <https://publications.parliament.uk/pa/ld5802/ldselect/ldjust-hom/180/18002.htm>.
- 3 In ‘Goldilocks and the three “Ts”’ bespreekt Sherman (2022) aan welke voorwaarden legitiem politieoptreden moet voldoen. We hebben voor dit artikel deze voorwaarden aangevuld met een vierde handvat.
- 4 <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206>.
- 5 <https://digital-strategy.ec.europa.eu/en/library/ethics-guide-lines-trustworthy-ai>.

Voordat we deze handvatten bespreken, gaan we eerst in op wat er allemaal speelt op het gebied van algoritmes binnen de politie.

Van voorspellen naar terugkijken

Toepassingen van algoritmes kunnen worden ingedeeld in drie typen:

1. algoritmes die ondersteunen met vooruitkijken,
2. algoritmes die ondersteunen in het nu, en
3. algoritmes die ondersteunen met terugkijken.

Vooruitkijkende algoritmes zijn het meest bekend. Dit zijn veelal algoritmes die gebruik maken van big data, afkomstig uit zowel open bronnen als politiebronnen, om een inschatting te maken over toekomstig crimineel gedrag. Dit wordt *predictive policing* genoemd. Er zijn hierbij meerdere zaken die voorspeld kunnen worden zoals criminaliteit in bepaalde gebieden, maar het kan ook gaan over inschattingen of personen extra kans maken om betrokken te raken bij een strafbaar feit (Perry et al., 2013). In Nederland wordt landelijk gewerkt met het Criminaliteits Anticipatiesysteem, dat op gebiedsniveau voorspelt waar en wanneer een verhoogde kans bestaat dat bepaalde vormen van criminaliteit kunnen voorkomen. Soortgelijke systemen worden ook gebruikt in andere Europese landen, waaronder Duitsland (KrimPro) en Italië (KeyCrime).

Algoritmes worden ook gebruikt om de politie in het hier en nu (*real time*) te ondersteunen. Deze algoritmes kunnen worden ingezet om menselijke capaciteit te verlichten en het politiewerk te versnellen, maar ook om informatie te verwerken die met enkel menselijke inzet niet meer (tijdig) is te verwerken. Zo helpen ANPR-camera's bij het automatisch

herkennen van kentekens. Die camera's kunnen ook een rol spelen bij de aanhouding van verdachten, zoals bij de aanslag op Peter R. de Vries. Ook zijn er zoekalgoritmes die de operatie ondersteunen door automatisch relevante informatie overzichtelijk aan te bieden, waaronder BlueSpot en BasisVoorziening Informatie voor Integrale Bevraging (BVI-IB) (Oosterheert, 2017). Een ander actueel voorbeeld van *real time* ondersteuning is crowdmanagementtechnologie, dataverzameling in de openbare ruimte via algoritmes en sensoren om de veiligheid te verbeteren.

Als laatste worden algoritmes ingezet voor toepassingen die terugkijken in het verleden. Het gaat hierbij bijvoorbeeld om toepassingen in rechercheonderzoek, vooral als er grote hoeveelheden data moeten worden geanalyseerd. Zo wordt gebruik gemaakt van *deep learning* algoritmes bij het lezen van miljoenen onderschepte *Encrochat*-berichten van criminelen. Deze worden nu ook gebruikt in het Marengo-proces. Een ander voorbeeld is het computersysteem HAVANK, dat helpt bij het vinden van een match tussen vingerafdrukken op een plaats delict en een database van veroordeelden en verdachten. Ook gebruikt de politie het gezichtsherkenningssysteem CATCH, dat het gelaat van verdachten vergelijkt met een database van ruim een miljoen mensen.

Vier handvatten voor betrouwbare toepassing

In de samenleving is er steeds meer aandacht voor de risico's van algoritmes in het politiewerk, van het probleem van vuile data tot discriminatie van minderheden (Schuilenburg & Soudijn, 2021). Het is daarom tijd voor een algemeen afwegingskader om de bruikbaarheid van algoritmes en de maatschappelijke effecten hiervan te toetsen. Vier handvatten kunnen de politie hierbij ondersteuning bieden.

1. Targeted: staat de werking van de toepassing in verhouding tot de opbrengst ervan?

De mogelijkheden van algoritmische toepassingen lijken ongekend. Studies laten zien dat dergelijke toepassingen kunnen leiden tot snellere en effectievere werkprocessen (WRR, 2016;

Algemene Rekenkamer, 2021). Toch moet hier worden gewaakt voor techno-trionfalisme. Automatisering via algoritmes wordt dan niet gezien als een veelbelovend middel, maar veeleer als ‘de’ oplossing voor het voorkomen en bestrijden van criminaliteit (Morozov, 2013). Dit gaat gepaard met torenhoge en vaak irreële verwachtingen over de voordelen van algoritmische toepassingen. In de praktijk is meer nuchterheid geboden. In dynamische omgevingen vallen de prestaties van deze toepassingen vaak tegen. De afhankelijkheid van techniek kan ertoe leiden dat zaken als ‘intuïtie’ en ‘kennis van de buurt’ in het politiewerk verloren gaan en dat er een ‘digitale bureaucratie’ wordt opgetuigd waarin de menselijke maat dreigt te verdwijnen (Peeters & Schuilenburg, 2018). Dan eroderen algoritmische toepassingen de menselijke omgang, tussen politie en mensen in de wijk bijvoorbeeld, omdat het vertrouwen in blackboxsystemen doorslaggevend wordt en er geen oog meer is voor de buitenwereld. Dergelijke effecten van digitale innovaties worden vaak onderschat. Zo wordt veel verwacht van beslisalgoritmes die handelingen kunnen automatiseren waardoor de menselijke tussenkomst van politieagenten niet langer noodzakelijk is. Dit was een van de redenen voor sluiting van politiebureaus in de Duitse deelstaat Baden-Württemberg. Maar uit onderzoek bleek dat dit een negatief effect had op het aantal woninginbraken en autodiefstallen; dat liet daarna juist een stijging zien (Blesse & Diegman, 2022). Je moet je dus telkens afvragen: is de meerwaarde van de digitale toepassing groter dan die van andere, analoge toepassingen?

2. Tracked: is de toepassing in overeenstemming met relevante juridische en ethische vereisten?

Bij de inzet van algoritmes in het politiewerk moeten nationale wetgeving en grondrechten worden nageleefd. Zo beoordeelt de politie of er bij het ontwerp en toepassing ervan wordt voldaan aan de eisen op het gebied van privacy in de Politiewet en de Wet Politiegegevens. Maar ook internationale regels zijn bindend voor het ontwerp en gebruik van algoritmische toepassingen, van de verdragen van de Europese Unie tot het secundaire EU-recht. Zo komt de laatste jaren de ene na de andere



Neem gebruikers en burgers mee in de ontwikkeling van algoritmische toepassingen

wet op het gebied van data en privacy uit de koker van de Europese Unie.

De Europese Unie – en dit is anders als in de Verenigde Staten en China – vervult steeds meer een regierol voor wet- en regelgeving met betrekking tot de digitalisering van de politiefunctie. Deze wet- en regelgeving hebben directe consequenties voor het politiewerk. Zo heeft de Europese Commissie, die verantwoordelijk is voor Europese wet- en regelgeving, een groot aantal juridische kaders op het gebied van big data en algoritmes opgesteld. Met betrekking tot de rechtshandhaving heeft de Commissie in de *Artificial Intelligence Act* (AI Act) een indeling gemaakt tussen vier AI-systemen waarbij geldt dat er striktere regels gelden naarmate het risico dat de technologie met zich meebrengt, groter is. Gelet op de grote risico's is het gebruik van *real time* biometrische systemen voor identificatie in de openbare ruimte met het oog op de rechtshandhaving verboden, met uitzondering van een beperkt aantal gevallen. Daarnaast zijn in de AI Act strikte eisen gesteld aan algoritmische toepassingen die onder meer worden gebruikt voor (i) het voorspellen van een daadwerkelijk of potentieel strafbaar feit, (ii) de profilering van personen tijdens de opsporing van strafbare feiten en (iii) misdaadanalyses waarmee grote hoeveelheden data worden doorzocht om onbekende patronen op te sporen of verborgen relaties te ontdekken.⁴

Naast wetsgrenzen moet worden gelet op ethische grenzen bij algoritmische toepassingen. Publieke organisaties als de politie dienen bij de inzet ervan immers publieke waarden te beschermen. Ook hierbij laat de Europese Unie zich steeds nadrukkelijker gelden met betrekking tot politieprojecten waarin gebruik wordt gemaakt van algoritmes. Zo heeft de



Literatuur

- Algemene Rekenkamer (2021). *Aandacht voor algoritmes*. Den Haag.
- Blesse, S. & Diegman, A. (2022). The place-based effects of police stations on crime: Evidence from station closures, *Journal of Public Economics*, www.sciencedirect.com/science/article/pii/S004727272200007X.
- Mali, B., Bronkhorst-Giesen, C. & den Hengst, M. (2017). *Predictive policing: lessen voor de toekomst*. Apeldoorn: Politie-academie.
- Mohler, G.O., et al. (2015). Randomized Controlled Field Trials of Predictive Policing, *Journal of the American Statistical Association*, 110(512), 1399–1411.
- Morozov, E. (2013). *To save everything, click Here*. New York: Public Affairs Books.
- Oosterheert, A.J. (2017). *De business-intelligencestrategie in de politiepraktijk*, in: Den Hengst, M., ten Brink, T., & ter Mors, J. (eds.): *Informatiegestuurd politiewerk in de praktijk*, pp. 275–284. Deventer: Vakmedianet.
- Peeters, R. & Schuilenburg, M. (2018). Machine Justice: Governing Security Through the Bureaucracy of Algorithms, *Information Polity. An International Journal of Government and Democracy in the Information Age*, (23)3, 267–280.

High Level Expert Group on AI van de Europese Unie een overzicht van ethische beginselen opgesteld waaraan de ontwikkeling, installatie en het gebruik van algoritmische toepassingen moeten voldoen. Hierbij dienen de volgende ethische beginselen te worden nageleefd: (i) respect voor menselijke autonomie, (ii) preventie van schade, (iii) rechtvaardigheid en (iv) verantwoording.⁵ Naast ethische grenzen zijn er door de Europese Unie ook technische eisen gesteld, waaronder dat de technologie robuust en veilig moet zijn. Daarbij gaat het onder meer om zaken als non-discriminatie, respect voor de privacy, kwaliteit van de gegevens en verantwoording.

3. Talked: worden verschillende vormen van kennis betrokken bij het ontwerp en de inzet van de toepassing?

Het vraagstuk van algoritmes wordt nu vooral technologisch benaderd. Het gaat dan om technische kennis over ‘de snelheid’ waarmee big data kunnen worden verzameld en het type algoritme om die data te kunnen ontsluiten, van eenvoudige rule-based algoritmes tot complexere typen zoals machine learning – en varianten hierop als deep learning (of een combinatie ervan). Maar algoritmes hebben ook een sociale kant, waarbij zaken als ‘politiecultuur’ en ‘werkstijlen’ een belangrijke rol spelen. De wijze waarop de toepassing werkt, is immers sterk afhankelijk van hoe hiermee in de praktijk wordt omgegaan. Zo zal een politiemedewerker het gebruik van een nieuwe toepassing als nodig

en urgent moeten ervaren om de prestaties te verbeteren. Anders wordt er geen of minder gebruik van gemaakt. Het is daarom zaak de kennis en ervaringen van gebruikers in een zo vroeg mogelijk stadium te betrekken. Het gaat hierbij om wat de oude Grieken *phronèsis* noemden, praktische wijsheid. Politieagenten bijvoorbeeld beschikken door jarenlange ervaring over praktische kennis over het gebruik van surveillancetechnieken. Dit is een andere vorm van kennis als technische kennis. Maar ook deze vorm van kennis is waardevol omdat ze laat zien hoe – in de praktijk – technische toepassingen worden beleefd, met alle emoties en gevoelens die daarbij een rol spelen.

Naast het inzetten van andere vormen van kennis (‘epistemische inclusie’) gaat het om de vraag hoe de politie verschillende lagen binnen de samenleving meer kan betrekken bij het ontwerp en de inzet van algoritmische toepassingen. Dit is het vraagstuk van sociale inclusie. Dit zal mede afhankelijk zijn van de type toepassing en het doel waarvoor ze wordt gebruikt. Maar vanuit het oogpunt van transparantie en proportionaliteit (*Tracked*) is het raadzaam om een zo divers mogelijk team van professionals en burgers mee te nemen bij het ontwerp van nieuwe toepassingen. Dit is belangrijk omdat zo stem kan worden gegeven aan iedereen wie dat onvoldoende heeft, waaronder jongeren en minderheden. Tegelijk kan hierdoor de acceptatie bij de burger van nieuwe technologie worden vergroot, bijvoorbeeld bij het gebruik van sensoren in

een wijk om inbraken te voorkomen. Dit alles betekent: ontwikkel algoritmische toepassingen met interdisciplinaire teams en neem daarin gebruikers en burgers mee. Differentieer hierbij in de manier waarop de toepassing wordt uitgelegd, omdat verschillende groepen andere belangen, aandachtspunten en kennisniveaus hebben.

4. **Tested: is de toepassing getest en effectief bevonden met de soorten doelen waar de toepassing voor wordt gebruikt en vindt hiervan periodieke evaluatie plaats?**

Politiewerk moet bij voorkeur bewezen werkzaam zijn en nut hebben. Dit geldt ook voor de algoritmes die hiervoor worden gebruikt. Dit is belangrijk voor zowel de acceptatie in de politieorganisatie als de daadwerkelijke resultaten die worden bereikt met het gebruik ervan. De wijze waarop technologie wordt uitgelegd en hoe ze wordt gepresenteerd als toegevoegde waarde voor het politiewerk door het management, is hierbij van groot belang. Vooral bij zelflerende algoritmes speelt het risico dat de uitkomsten worden gepresenteerd als absolute waarheid door een schijn van objectiviteit – wat vaak niet het geval is. Dit kan ertoe leiden dat politieprofessionals ofwel het advies onterecht overnemen en blind hierop vertrouwen, of dat de adviezen en uitkomsten worden genegeerd als er niet aan de belofte van volledig juiste adviezen wordt voldaan.

Het gepresenteerde beeld moet daarnaast overeenkomen met de veiligheidseffecten die hiermee worden bereikt. Dit is niet altijd eenvoudig om aan te tonen. Een goed voorbeeld hiervan zijn – wederom – zelflerende algoritmes. De ‘logica’ van deze algoritmes is nooit af en daarom moet er continu aandacht zijn voor de manieren waarop ze zich blijven ontwikkelen en de effecten die ze sorteren. Dit betekent dat er een frequente evaluatie nodig is van de werking van algoritmes, en moet men ervan bewust zijn dat dit sterk contextafhankelijk kan zijn. Zo laten evaluaties van *predictive policing* wisselende – en soms zelfs tegenstrijdige resultaten zien. In een aantal Amerikaanse steden bleek het toepassen hiervan effectief, in andere landen, waaronder Nederland, is er geen aantoonbaar effect aangetoond op het niveau van de criminaliteit (o.a.



Politieagenten beschikken door jarenlange **ervaring** over praktische **kennis** over het gebruik van **surveillancetechnieken**

Mohler et al., 2015; Mali, Bronkhorst-Giesen & den Hengst, 2017; Ratcliffe et al., 2021).

Tot slot moet niet alleen worden gekeken of algoritmes de juiste analyse doen, maar ook hoe die vervolgens worden gebruikt in de praktijk door professionals. Het gebruik van technologie is namelijk sociaal en cultureel bepaald en is afhankelijk van de inbedding in de organisatieprocessen. Hierdoor kan het gebruik van algoritmes, en daarmee de effecten die worden bereikt, door de tijd heen veranderen. Vandaar dat er niet één evaluatiemoment van algoritmische toepassingen moet zijn, maar dat dit idealiter een continu proces is binnen de politie.

Naar de toekomst

De Strategische Agenda Politie (2021-2025) stelt dat *state-of-the-art* technologie van wezenlijk belang is voor het politiewerk. Op steeds meer gebieden kiest de Nederlandse politie voor algoritmische toepassingen, van het werk op straat tot de opsporing en recherche. Op dit moment is er geen algemeen afwegingskader voor verantwoorde en betrouwbare ontwikkeling en gebruik van algoritmes. In dit artikel hebben we vier handvatten hiervoor gegeven. Zo moet de inzet in verhouding staan tot de opbrengst ervan, waarbij ook wordt gekeken naar alternatieve (analoge) oplossingen. Naast nationale wetgeving moet er worden getoetst aan Europese ethische en juridische kaders. Ook is het nodig om professionals en burgers via multidisciplinaire teams te betrekken bij de ontwikkeling en inzet van algoritmische toepassingen. Tot slot dienen er meerdere (periodieke) evaluatiemomenten te zijn waarmee de veranderingen van de effecten ervan worden beoordeeld.

- Perry, W.L. et al. (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Santa Monica, CA: RAND Corporation.
- Ratcliffe, J.H. et al. (2021). The Philadelphia predictive policing experiment. *Journal of Experimental Criminology*, 17(1), 15-41.
- Saunders, J., Hunt, P., & Hollywood, J.S. (2016). Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot. *Journal of Experimental Criminology*, 12(3), 347-371.
- Schuilenburg, M. & Soudijn, M. (2021). Big data in het veiligheidsdomein: Onderzoek naar big data-toepassingen bij de Nederlandse politie en de positieve effecten hiervan voor de politieorganisatie. *Tijdschrift voor Veiligheid*, 20(4), 44-62.
- Sherman, L.W. (2022). Goldilocks and the three "Ts": Targeting, testing, and tracking for "just right" democratic policing. *Criminological Public Policy*, 21, 175-196.
- WRR (2016). *Big Data in een vrije en veilige samenleving*. Den Haag.