Hoe AI de opsporing én de misdaad verandert

Dubbelspel met data

AI helpt de politie bij het oplossen van misdaden, maar gaat net zo makkelijk zelf het boevenpad op. De voordelen, haken en ogen van kunstmatige intelligentie voor politie, criminelen en slachtoffers.

TEKST: CARLIJN SIMONS

JOE BUGLEWICZ NYT/ANP, BEWERKING QUEST

Uit privacyoverwegingen mag de politie in Nederland voor gezichtsherkenning alleen gebruikmaken van een database met foto's van verdachten en veroordeelden.

‘Auto’s, telefoons, elektrische tandenborstels en robotstofzuigers: alles produceert data’

De Duitse politie test een robothond die onderzoek kan doen in rampgebieden en op gevaarlijke plaatsen delict naar sporen zoekt.

MAREN WINTER/ALAMY

Het was in juli 2020 een van de grootste klappers die de politie ooit maakte. Met het hacken van chatdienst EncroChat, de WhatsApp van de onderwereld, kon justitie meelezen met de berichtjes die criminelen elkaar stuurden. Die waanden zich onbespied dankzij hun Pretty Good Privacy-telefoon (PGP), een smartphone zonder camera, microfoon of gps. Alleen ontvanger en verzender konden de versleutelde berichten lezen. Dachten ze. Dus communiceerden ze vrijelijk over hun duistere zaakjes. Daarmee wierpen ze de politie een schat aan informatie in de schoot, die na de inzet van AI leidde tot een forse buit: onder meer twintig miljoen euro cash, 8000 kilo cocaïne, negentien synthetische-drugslabs, tientallen vuurwapens en honderd verdachten van zware misdrijven. Dat was de moeite meer dan waard. Maar hoever kan de politie gaan met het combineren van data?

Speurende computer

In de slordige 25 miljoen berichten die de politie wist te kraken, spraken de criminelen in bedekte termen als ‘broodjes halen’ en ‘slapen’ over onder meer drugsdeals en liquidaties. Maar als je weet dat iemand die zich Piet Costa noemt met een handlanger babbelt over het smokkelen van een partij cocaïne, heb je nog geen zaak. Dus liet de politie een slimme zoekmachine los op alle gegevens om de berichtjes met waardevolle informatie eruit te filteren. Een ander intelligent systeem combineerde die resultaten met aanvullende data uit zaken als lopende dossiers, observaties, locatie-informatie en posts op sociale media.

Zo maakt de politie op allerlei manieren handig gebruik van kunstmatige intelligentie (zie het kader ‘Technische recherche’). ‘Bijvoorbeeld met een beeldherkenningssysteem’, vertelt Daniël Stuart, projectmanager AI bij de politie. ‘Dat kan met goede betrouwbaarheid de cijfers en letters van kentekens invullen, als die op een foto niet duidelijk leesbaar zijn. En we gebruiken een semantisch taalmodel dat data doorzoekt. Daarmee kun je een dossier niet alleen doorspitten op de term ‘gouden ketting’, maar automatisch ook op woorden als ‘erfstuk’ en ‘sieraad’.’ Behalve in de opsporing doen slimme computermodellen ook dienst op straat. Zo hebben agenten een speciale smartphone met allerhande apps, die hen toegang verschaffen tot verschillende informatiesystemen. Dan kan een surveillant die iemand aanhoudt voor een verkeersovertreding met een druk op de knop zien of diegene ooit een vuurwapen heeft gebruikt, of misschien nog een belastingschuld heeft.

Digitaal spoor

AI maakt het stukken gemakkelijker om gebruik te maken van de steeds grotere hoeveelheden gegevens die beschikbaar zijn om criminelen te pakken. ‘Van telefoons en computers tot auto’s en zelfs robotstofzuigers en elektrische tandenborstels: alles produceert data’, zegt Marc Schuilenburg. Hij is hoogleraar Digital Surveillance aan de Erasmus Universiteit Rotterdam en doet veel onderzoek naar de rol van AI, big data en algoritmen in veiligheid.

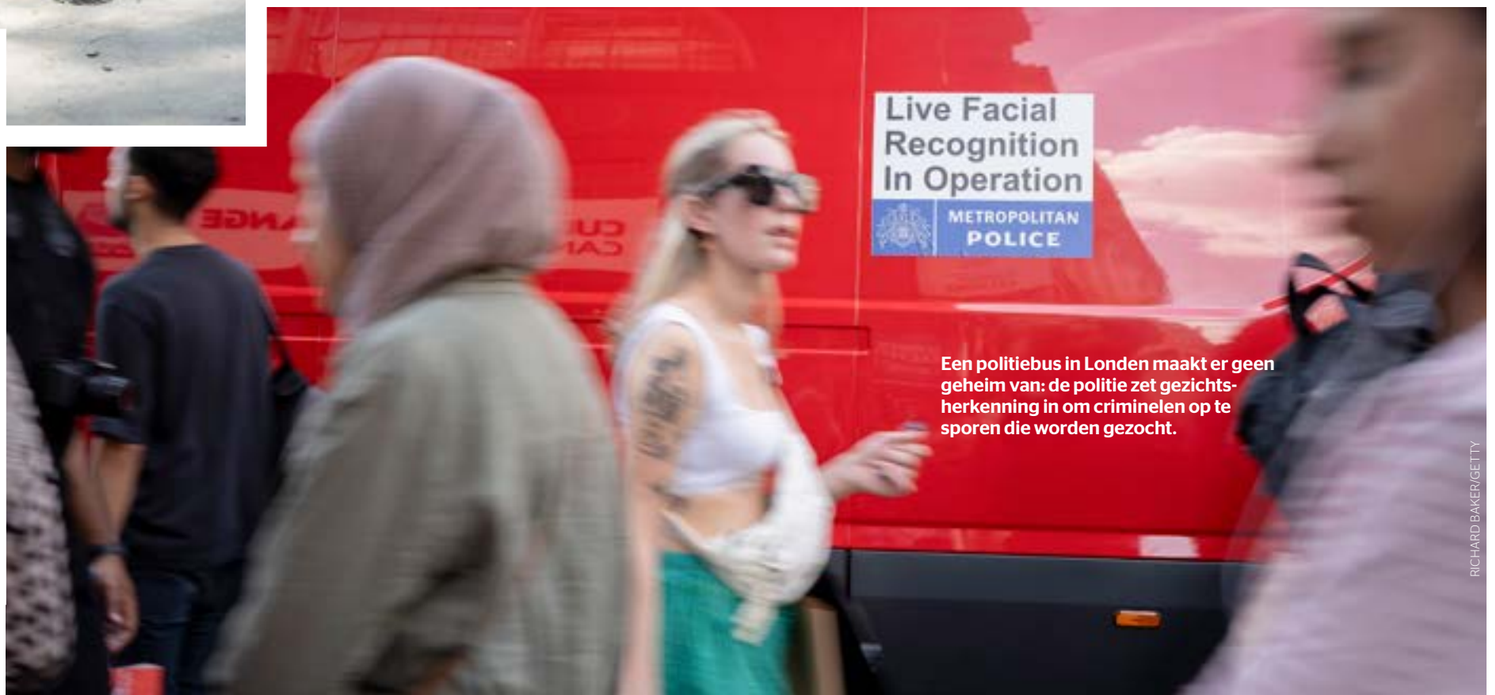
‘Die digitalisering is echt een gamechanger in de misdaadbestrijding. De politie kan intappen op die digitale sporen. Die leveren niet alleen meer, maar ook veel rijkere en gevarieerdere data op dan de gegevens van de politie zelf. Met de digitale deurbel die zo’n 1,2 miljoen Nederlanders bij hun voordeur hebben hangen, heeft ze er bijvoorbeeld

Voorspellen is niet genoeg

Het beloofde een zeer effectieve toepassing van AI te worden: een algoritme dat inschat waar en wanneer de kans op een veelvoorkomende misdaad het grootst is. Het deed dat op basis van gegevens uit politiebestanden (aangiftes en criminaliteitscijfers), het CBS (leeftijd, geslacht, aantal uitkeringen, gezinssamenstelling) en de aanwezigheid van bijvoorbeeld scholen, cafés, winkels en op- en afritten naar snelwegen. Als je het risico op bijvoorbeeld een woninginbraak kunt taxeren, kan de politie daar gericht op reageren, was het idee. Toen de politie het Criminaliteits Anticipatie Systeem (CAS) in 2015 in gebruik nam, ging ze ervan uit 40 procent van de woninginbraken en 60 procent van de straatroven te kunnen voorspellen. Toch concludeerde sociaal wetenschapper Bas Mali van de Politieacademie twee jaar later dat CAS geen aantoonbaar effect had op de opsporing en misdaadbestrijding. Dat had volgens hem niet per se met het systeem te maken. ‘Om effectief te zijn is het ook noodzakelijk om te begrijpen waarom de kans op criminele activiteit in een bepaald gebied en op een bepaald tijdstip hoog is.’ Die inzichten kun je vertalen naar concrete werkopdrachten. Maar die vertaalslag is nooit gemaakt. ‘Een voorspelling is één stap, maar die leidt tot niets als er niets mee wordt gedaan’, schreef Mali in zijn rapport. Omdat CAS in combinatie met andere informatie wel meerwaarde heeft, maakt de politie er wel nog steeds gebruik van.

Nieuwe misdaad

Al jaren nemen de misdaadcijfers in Nederland af. Volgens de Veiligheidsmonitor 2023, een onderzoek van het Centraal Bureau voor de Statistiek (CBS), zijn er sinds 2005 53 procent minder mensen slachtoffer van traditionele, offline criminaliteit. Dat zijn bijvoorbeeld geweldsdelicten, inbraak, diefstal en vernielingen. Online neemt misdaad juist toe. In 2023 viel 16 procent van de Nederlanders ten prooi aan zaken als online bedreiging, oplichting en intimidatie. Met name hacken (waarbij iemand met kwade bedoelingen inbreekt op een apparaat, e-mail- of bankaccount) en aankoopfraude (je koopt iets op internet dat niet wordt geleverd) kwamen vaak voor. In totaal kreeg twee derde ook ten minste één telefoontje, e-mail of een ander bericht dat (waarschijnlijk) van een oplichter was. Zoals iemand die zich voordeed als bankmedewerker. Gelukkig trapte maar twee procent erin. Naar verwachting gaat AI een steeds grotere rol spelen in zulke onlinecriminaliteit.



Een politiebus in Londen maakt er geen geheim van: de politie zet gezichtsherkenning in om criminelen op te sporen die worden gezocht.

RICHARD BAKER/GETTY

AI heeft het gedaan

Het liep in 2023 met een sisser af, toen bekend werd dat sommige van de artikelen van het Amerikaanse tijdschrift *Sports Illustrated* waren geschreven door ChatGPT. Behalve lezers die zich bedrogen voelden, had niemand er schade van ondervonden. Maar stel dat dat wel het geval was geweest: wie had je daarvoor dan aansprakelijk kunnen houden? ‘Sommige vormen van AI-criminaliteit kunnen met het huidige strafrecht worden aangepakt’, zegt hoogleraar Digital Surveillance Marc Schuilenburg. ‘Afpersing, computervredebreuk en oplichting bijvoorbeeld. Het wordt ingewikkelder als AI zelf strafbare feiten pleegt doordat het systeem zelfstandig beslissingen neemt.’ Zo kan een model dat is getraind met data die niet objectief zijn de ene bevolkingsgroep boven de ander stellen en tot stafbare discriminerende besluiten komen. ‘Maar wie is de dader? De persoon die het zelflerende algoritme heeft ontworpen? Het bedrijf achter het AI-systeem? Of het algoritme zelf?’ Het zijn vragen waarop niemand nog een sluitend antwoord heeft.

AI-systemen helpen de politie, maar zijn ook een aantrekkelijk doelwit voor criminelen

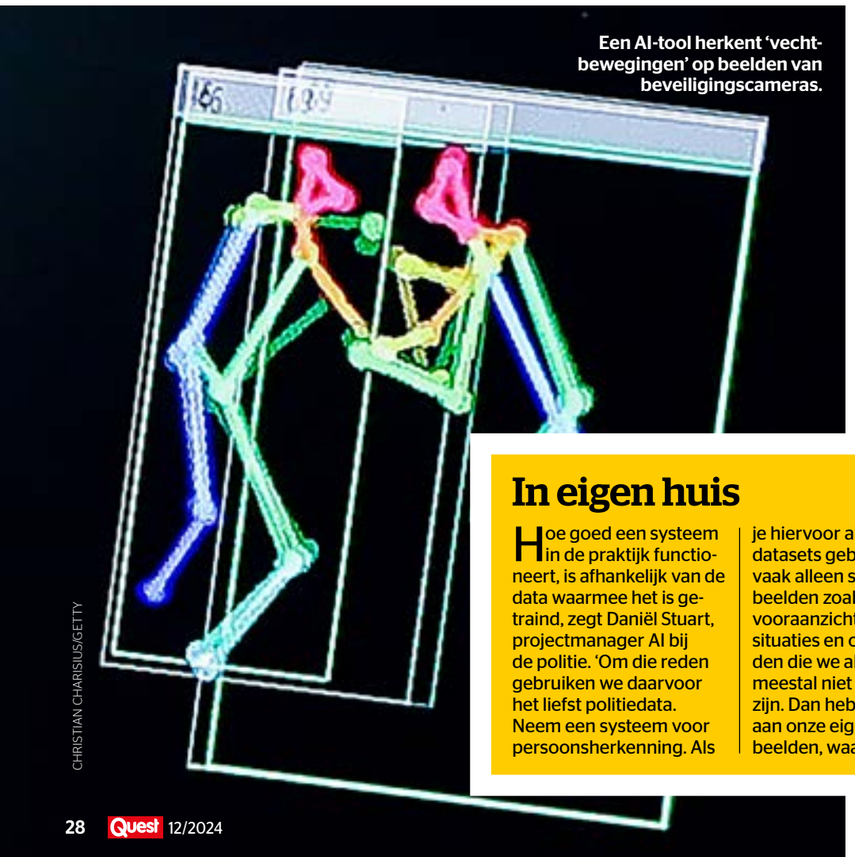
Pas op de plaats

Kunstmatige intelligentie helpt om efficiënt de veiligheid in de samenleving te vergroten. 'Efficiëntie en veiligheid zijn twee belangrijke publieke waarden', zegt hoogleraar Digital Surveillance Marc Schuilenburg. 'Maar dat zijn het recht op privacy en non-discriminatie ook. Evenals transparantie en accountability, wat betekent dat te achterhalen en uitlegbaar moet zijn waar een systeem zijn data vandaan heeft, hoe het werkt en beslist. Met AI-systemen die steeds zelfstandiger beslissingen nemen, moeten juist die waarden een belangrijke rol spelen in het ontwerp van de modellen.'

Recht op privacy: informatie over personen helpt bij het opsporen van verdachten. Maar je kunt niet zomaar van iedereen bijvoorbeeld camerabeelden maken. Een opsporingsmethode zoals automatische gezichtsherkenning is daarom (tot nu toe) beperkt tot een database met foto's van verdachten en veroordeelden.

Non-discriminatie: een AI-systeem is getraind met enorme hoeveelheden data. Algoritmen doen op basis daarvan voorspellingen. Het risico bestaat dat er discutabele aannames worden gedaan als de gegevens waarmee het systeem is getraind niet objectief zijn. Zoals gebeurde in het toeslagenschandaal.

Transparantie en accountability: je moet weten welke AI-systemen je gebruikt, met welke data die zijn getraind en hoe ze werken. Apps en algoritmen mogen geen black box zijn waarvan niemand een idee heeft hoe ze tot hun uitkomsten komen, maar moeten dus open en transparant zijn.



Een AI-tool herkent 'vechtbewegingen' op beelden van beveiligingscameras.

CHRISTIAN CHARISIUS/GETTY

In eigen huis

Hoe goed een systeem in de praktijk functioneert, is afhankelijk van de data waarmee het is getraind, zegt Daniël Stuart, projectmanager AI bij de politie. 'Om die reden gebruiken we daarvoor het liefst politiedata. Neem een systeem voor persoonsherkenning. Als je hiervoor algemene datasets gebruikt, heb je vaak alleen standaardbeelden zoals rechte vooraanzichten. Terwijl de situaties en omstandigheden die we als politie zien meestal niet standaard zijn. Dan hebben we meer aan onze eigen camerabeelden, waarop mensen bijvoorbeeld van boven staan, om het AI-model te verfijnen. Dat maakt het geschikter voor ons werk.' De Nederlandse politie ontwikkelt, in tegenstelling tot veel andere landen, veel AI-systemen zelf. 'Dan weten we met welke data het is gevoed en hoe het presteert.'

potentieel 1,2 miljoen camera's bij. Of neem het bewakingssysteem van een Tesla: die maakt opnamen van mensen die een poging doen om de auto te stelen.'

Nu is het natuurlijk niet te doen om al die data met de hand door te ploegen om de gouden aanwijzing te vinden. Hoeft ook niet: AI analyseert de gegevens moeiteloos en razendsnel. Bovendien kan kunstmatige intelligentie allerlei patronen ontdekken, waar een mensenbrein misschien niet op komt. Bewijs verzamelen en het opsporen van verdachten gaan daardoor niet alleen rapper en makkelijker, maar ook effectiever en beter. 'Zoals in de EncroChat-zaak', vertelt Schuilenburg. 'Opeens wist de politie wie contact had met wie, over welke drugs dat ging, waar die binnenkwamen en wie wat deed. Dat verschafte haar zicht op criminele netwerken als nooit tevoren, waardoor ze tot allerlei nieuwe verbanden, inzichten en conclusies kwam.' Met een golf aan arrestaties tot gevolg, zoals die van Roger P., alias Piet Costa, als spil in een omvangrijk drugsnetwerk.

Voor het grijpen

Tegenvaller is dat criminelen tegelijkertijd ontdekken dat kunstmatige intelligentie ook een handig instrument voor hun eigen louche activiteiten kan zijn. Want ChatGPT schrijft net zo makkelijk een professionele tekst die vraagt om snel geld over te maken, of om belangrijke persoonlijke gegevens te delen. Ook erg populair zijn deepfakes, waarbij samengevoegde beelden een niet van echt te onderscheiden nieuw beeld creëren. 'Een misdadiger kan zo'n deepfake vervolgens gebruiken voor strafbare zaken als fraude, misleiding of afpersing.' Zo dreef een door AI gemaakte advertentie met een voorstelling van presentator Jort Kelder goedgelovige investeerders recht in de handen van listige bitcoinfraudeurs.

In de Chinese stad Hangzhou houdt AI met slimme camera's de wegen in de gaten. Het systeem Tianyao spot ongelukken en overtredingen met een nauwkeurigheid van 95 procent en waarschuwt de politie binnen 20 seconden. Dat scheelt de verkeerspolitie patrouilleren. Maar als criminelen de boel platleggen, kijkt er niemand meer naar de straten...

ALAMY

ALAMY

Technische recherche

AI heeft in opsporingswerk allerlei verschijningsvormen. Een greep:

Deepfake: de deepfakevideo van Sedar Soares die de Nederlandse politie in 2022 maakte, was een wereldprimeur. Soares, die in 2003 op 13-jarige leeftijd werd vermoord, roept in het filmpje iedereen die meer weet op zich te melden. Helaas nog zonder resultaat.

Big data analytics: mobieltjes, tablets, usb-sticks, laptops, servers en harddisks staan vol informatie die van belang kan zijn in een onderzoek. Hansken heet het systeem dat met een snelheid van drie terabytes per uur tekst, video, audio en locatiedata opslaat, labelt en doorzoekbaar maakt.

Cyber agent technology: Sweetie, de AI-chatbot van Terres des Hommes, ging op internet het gesprek aan met mensen die seksuele interesse toonden in kinderen. Het doel? Verdachte personen identificeren en die waarschuwen of vervolgen. Er is bij deze AI-inzet wel mogelijk sprake van uitlokking, en dat mag niet volgens de Nederlandse wet. De politie zet dan ook nog geen chatbots in om zedendelinquenten op het spoor te komen.

Daarbovenop lopen AI-systemen het risico om slachtoffer te worden van criminaliteit. Omdat ze een steeds grotere rol spelen in de samenleving, heeft het illegaal in de war schoppen ervan potentieel catastrofale consequenties. 'Neem een terrorist die het systeem waarop zelfrijdende auto's werken hackt en dat dan programmeert om een aanslag mee te plegen', schetst Schuilenburg een toekomstscenario. 'Of de aandelenmarkt, waarop de handel nu al voor een groot deel wordt bestierd door algoritmen. Sabotage daarvan kan geautomatiseerde beslissingen beïnvloeden, met misschien grote gevolgen voor de economie.' Voor dit soort misdaden hoef je als crimineel niet eens een goed stel hersens te hebben. 'Voor veel AI-tools is technische kennis van zaken helemaal niet nodig. Bovendien is die software vaak gratis en vrij toegankelijk.'

Wees gewaarschuwd

'Dat maakt het voor criminelen aantrekkelijk om AI in te zetten', zegt Daniël Stuart. Dus hoewel de misdaadcijfers verder op alle fronten dalen (zie het kader 'Nieuwe misdaad' en het artikel op pagina 10 van deze *Quest*), maakt de politie zich op voor een boevenjacht die steeds meer via computers plaatsvindt. Zo is het leren herkennen van deepfakes met behulp van AI een van de hoogste prioriteiten.

'Tot nu toe gaat het om relatief eenvoudige toepassingen bij de bestrijding en het voorkomen van criminaliteit', zegt Schuilenburg. 'Zoals apps met simpele algoritmen of systemen die grote datasets combineren en doorzoeken. Maar dat zal waarschijnlijk snel veranderen. In de toekomst wordt naar verwachting meer en meer gebruikgemaakt van complexere AI-modellen. Je kunt daarbij denken aan biometrische vormen van gezichtsherkenning (meetbare kenmerken waarmee je iemand kunt identificeren, zoals iris- en vingerdrukherkenning, red.) om de identiteit van personen vast te stellen of volledig zelflerende algoritmen die op eigen initiatief verbanden leggen.'

Dat werkt efficiënt en vergroot de veiligheid, maar brengt ook gevaren met zich mee (zie het kader 'Pas op de plaats'). Want hoe zit het met het recht op privacy als politiesoftware gezichten gaat herkennen? En hoe voorkom je dat zo'n zelflerend algoritme discriminerende beslissingen neemt? Want terwijl criminelen elke regel aan hun laars kunnen lappen, is de politie gebonden aan de grenzen die EU-richtlijnen en de Nederlandse wet stellen, erkent Stuart. 'Zo moeten wij eerst de gevolgen voor grondrechten beoordelen voordat we een systeem kunnen invoeren.' Aan de andere kant herinnerde de EncroChat-zaak criminelen er op pijnlijke wijze aan dat je nooit zeker kunt weten dat de politie niet op je systeem kan inbreken. Wat dat betreft zullen agenten en criminelen ook in een AI-gedreven toekomst elkaar het leven zuur blijven maken. En voor geen van beide zal het ooit 'game over' zijn. ■

redactie@quest.nl