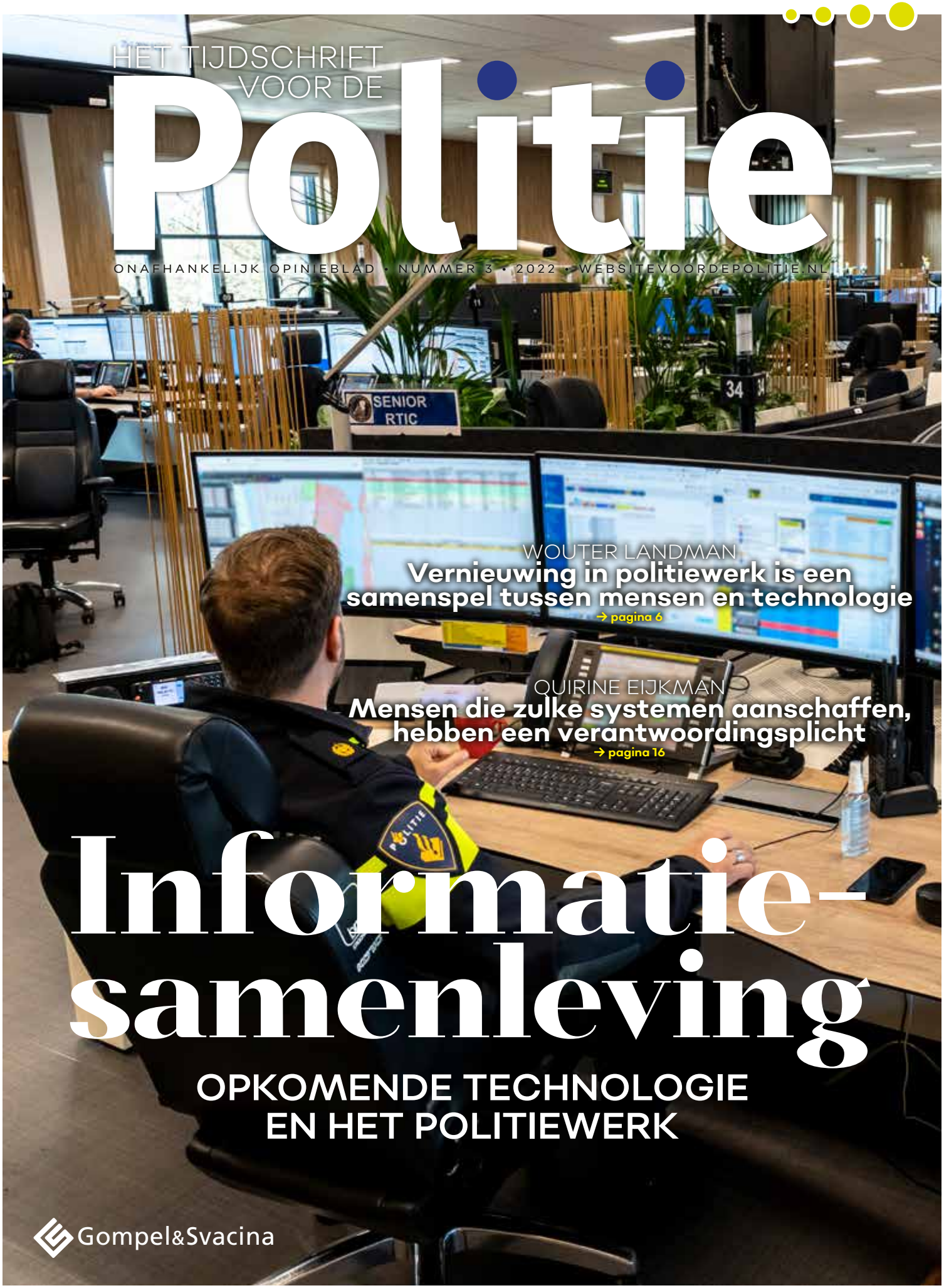
HET TIJDSCHRIFT VOOR DE

Politie

ONAFHANKELIJK OPINIEBLAD • NUMMER 3 • 2022 • WEBSITEVOORDEPOLITIE.NL



Informatie-samenleving

OPKOMENDE TECHNOLOGIE EN HET POLITIEWERK

Gompel&Svacina

Kwalitatief hoogwaardig functionele schoenen voor WERK & VRIJE TIJD!

Verkrijgbaar bij uw vakman of in de HAIX® Webshop

haix.nl

Politiewerk is mensenwerk

De samenleving informatiseert en digitaliseert in razend tempo. We zien het, wereldwijd. De ontwikkelingen zijn nauwelijks bij te houden. Dat vraagt – ook voor de politie – doordachte ontwikkeling van strategie. De commissie-Schneiders zegt dat de landelijke eenheid – en dus het hele korps – grote aanpassingen moet doen om niet verder achter te lopen. In dit nummer kunt u lezen dat informatisering en digitalisering grote mogelijkheden bieden. Maar ook risico's kennen, niet in de laatste plaats op ethisch gebied.

De ontwikkelingen hebben grote invloed op de politieorganisatie. Werkprocessen worden anders en informatie is ook bij de politie 'het nieuwe goud'. Het besef wordt sterker dat daardoor ook het vak en het vakmanschap veranderen.

Tegelijkertijd is er de vraag wat digitalisering betekent voor de taak van politie. *Politie in Ontwikkeling* voegde veel eerder aan de geografische oriëntatie een nodale oriëntatie toe, een gerichtheid op *stromen en knooppunten*. Het aandachtsgebied breidt zich verder uit, nu naar het virtuele domein. Het recente working-paper *Politie in een veranderende samenleving* van de Wetenschappelijke Raad voor Regeringsbeleid (WRR) beschrijft 'het vrij algemene gevoel dat er nauwelijks wordt gehandhaafd op het internet, dat het internet *underpoliced* is'. Daar ligt een taak voor de politie, zo lijkt de WRR te suggereren. En na het internet doemen alweer eerste contouren op van de metaverse, daarover lezen we ook in deze editie.

Het gaat dus om vragen over vakmanschap *en* om betekenis en effect van politiewerk. Begin deze eeuw ging de politie informatiegestuurd (IGP) werken. Het denken over de betekenis van informatie kwam op gang. De enthousiastelingen zeiden: de politie is vooral een *informatieverwerkend bedrijf*: informatie wordt opgepikt, verwerkt, geanalyseerd, toegepast, uitgewerkt en neergelegd in documenten, waar uiteindelijk de rechtspraak hun beslissingen op baseert. Vanuit die gekozen bril is er niets tegen in te brengen. De ontwikkeling van informatisering en digitalisering gaat sindsdien verder en verder, technologisering en innovatie jagen dit verder aan.

Ik moet eerlijk zeggen dat ik me nooit volledig heb overgegeven aan het idee dat de politie vooral een *informatieverwerkend bedrijf* is. Alle gesprekken over de opgaves en uitdagingen die de steeds verder gaande informatisering en digitalisering met zich mee brengen, voelen bij mij ergens 'unheimisch' aan. Dat komt omdat het niet meer over mensen lijkt te gaan. Mensen lijken bijna een ondergeschikte factor te worden.

> Mensen lijken een **ondergeschikte** factor te worden

Eén van mijn basics is: politiewerk is mensenwerk, voor én door mensen. Voor de burgers, door politiemensen. Er is sprake van politiewerk als *mensen* onrecht wordt aangedaan of als *mensen* in de *knel* komen of dreigen te komen. Ook al gebeurt dat digitaal. Dan reageren *politiemensen*, wellicht gebruik makend van de nieuwste technieken – dat wel –, maar *in the end* geven *politiemensen* aandacht, luisteren ze en handelen ze. En dat wordt dan weer opgemerkt en gevoeld door de *burgers* die het aangaan. Die burgers waarderen dat er aandacht is voor hun situatie. Als het goed is, tenminste. En als het *niet* goed is, ligt dáár de opgave.

Een van mijn andere basics is dat politiewerk in de kern iets tijdloos heeft. Als het recht met voeten wordt getreden of als dat dreigt, als mensen ondanks alle inzet op het goede samenleven toch in crisis of in nood komen, dan ligt er een taak voor de politie. Het blijft in de eerste plaats om mensen draaien, mensen die samen leven. Vroeger, nu en in de digitale toekomst.

Jaco van Hoorn
Hoofdredacteur

HET TIJDSCHRIFT VOOR DE
Politie
NUMMER 3 • 2022

Foto: Bureau Landman

6

De opkomst van de politiemachine
Volgens Wouter Landman kan de kracht van de opkomende technologieën pas ten volle benut worden als de politieorganisatie loskomt van de bestaande routines en met verbeeldingskracht **nieuwe manieren van werken** realiseert.

Foto: Erasmus Universiteit, Rotterdam

11

Marc Schuilenburg en Martijn Wessels stellen vast dat er geen algemeen afwegingskader is voor verantwoorde en betrouwbare ontwikkeling en gebruik van **algoritmes**. Ze geven vier handvatten om dit aan te pakken.

Foto: Erik Laan Photoos, Haarlem

16

Nederland mensenrechtengidsland?
Volgens rechtssociologe **Quirine Eijkman** wordt die kwalificatie problematisch wanneer heel veel autoriteit wordt toebedeeld aan voorspellende systemen. Er zijn twee grote problemen: de mogelijkheid van discriminatie en dirty data.

Coverfoto
Politie.nl

Colofon

Nummer 3, jaargang 84

Verantwoordelijk uitgever
Mr. Stephan Svacina
Gompel&Svacina bv
Antwerpen / 's-Hertogenbosch
info@gompel-svacina.nl
www.gompel-svacina.eu

Hoofdredacteur
Drs. Jaco van Hoorn MPA

Redactie
Dr. Maud van Bavel; Marcel Bruinsma MBA; dr. mr. Barbara van Caem; mr. Sanne Groen; dr. Merlijn van Hulst; mr. dr. Wouter Jong; Evert Jan Kasteel EMSD; dr. Edwin Kruisbergen; dr. Wouter Landman; dr. Joery Matthys; dr. Marc Schuilenburg; dr. Annika Smit; dr. Ronald van Steden; prof. dr. Pieter Tops; mr. Hans de Vries

Eindredactie en redactieadres
Jan van Balkom MA
+31 (0)6 13470687
Achterstraat 95
5268 EB Helvoirt
jan.vanbalkom@gompel-svacina.nl

Boekenredactie en recensies
Dr. mr. Barbara van Caem
Alpen Rondweg 23
1186 CV Amstelveen

Foto: Pexels

25

Technologie biedt kansen om het politiewerk of de organisatie te verbeteren, versnellen of vergemakkelijken. Het **team Science en Technology** van de politie houdt bij welke technologieën en toepassingen een impact hebben op de verschillende aspecten van het werk van de politie.

Foto: VR Training Academy, Enschede

36

Metaverse

Het Rathenau Instituut heeft tien ontwerpeisen opgesteld voor veilige technologieën voor een digitale samenleving van morgen. Deze ontwerpeisen willen ze samen met belanghebbenden in de maatschappij uitwerken. Welke **rol** ziet de politie daarbij voor zichzelf?

En verder

Advertenties
Irene Schaddelee-Pesch
+31 (0)6 23700323
info@is-acquisitie.com

Abonnementen
Het Tijdschrift voor de Politie verschijnt vier keer per jaar en is gratis voor hoger opgeleide politiemensen.
Overheid/instelling/zakelijk: €174,-
Privépersoon: €88,-

Abonnementen lopen per kalenderjaar en worden automatisch verlengd, tenzij uiterlijk 30 dagen voor de vervaldatum bij onze abonneeservice wordt opgezegd.

Abonneren kan via www.website voordepolitie.nl of via onze abonneeservice.

Gompel&Svacina Abonneeservice
Postbus 105
2400 AC Alphen aan den Rijn
Tel. NL: 0031 (0)172476085
Tel. BE: 0032 (0)25888745
E-mail: TVP@spabonneeservice.nl

Gompel&Svacina

De opkomst van de politiemachine

OVER DE INVLOED VAN OPKOMENDE TECHNOLOGIEËN

Onze samenleving bevindt zich in de overgang naar de vierde industriële revolutie. Er komen nieuwe technologieën op die van invloed (zullen) zijn op de manier waarop we leven en werken. Deze opkomende technologieën zijn in de afgelopen jaren ook – veelal op kleine schaal – gebruikt in de politieorganisatie. In dit artikel verken ik de invloed hiervan op het politiewerk.

Over de auteur
Wouter Landman PhD begeleidt veranderprocessen en verricht onderzoek. Actuele thema's zijn: technologie & politiewerk, innovatie en ontwikkeling van politieteams.
www.bureaulandman.nl

Tekst: Wouter Landman • Foto: Roel Dijkstra

Politiewerk is altijd beïnvloed door technologische ontwikkelingen in de samenleving. Zo is de noodhulp van vandaag onder andere een uitvloeisel van de introductie van de politieauto gedurende de tweede industriële revolutie en van informatie- en communicatietechnologie tijdens de derde industriële revolutie. Op dit moment bevinden we ons aan het begin van de overgang naar de vierde industriële revolutie. Deze revolutie wordt gekenmerkt door een steeds verdere versmelting van de fysieke, biologische en digitale wereld. Deze versmelting is onder meer zichtbaar in robotisering van menselijke activiteiten. Artificiële intelligentie (AI) is de dragende technologie van de vierde industriële revolutie, vergelijkbaar met de verbrandingsmotor in de twintigste eeuw.[1]

Technologie en politiewerk

In de afgelopen tien jaar hebben de opkomende technologieën van de vierde industriële revolutie hun weg gevonden naar het politiewerk. Slimme camera's, het criminaliteitsanticipatiesysteem (CAS), de Raffinaderij, PublicSonar en andere software voor online monitoring, chatbots in de dienstverlening: het zijn voorbeelden van hoe de politie in Nederland gebruik maakt van opkomende technologieën in het politiewerk. In de komende jaren zal het gebruik van dergelijke technologieën in het politiewerk intensiveren en normaliseren. Een relevante vraag is of en op welke wijze het politiewerk hierdoor verandert dan wel gaat veranderen. Het antwoord op deze vraag kan nu niet worden gegeven, maar wel worden verkend. Dat doe ik in dit artikel.[2]

Politiewerk in vier vermogens

De invloed van technologie op politiewerk is op vele manieren te duiden. In dit artikel kies ik voor het perspectief van vermogens. Een vermogen is een combinatie van mensen,

middelen en methoden die bij de uitvoering van politietaken wordt ingezet. Ik maak onderscheid tussen vier vermogens en gebruik hierbij het menselijk lichaam als metafoor:

- De *ogen* van de politie representeren het surveillancevermogen. Met dit vermogen neemt de politie de voortdurende stroom van activiteiten in de samenleving waar.
- Het *brein* van de politie representeert het cognitieve vermogen. Met dit vermogen verwerkt de politie gegevens om zodoende tot bruikbare informatie te komen.
- De *tanden* van de politie representeren het fysieke vermogen. Met dit vermogen geeft de politie invulling aan haar 'sterke arm' die nodig is wanneer dwang moet worden toegepast.
- Het *hart* van de politie representeert het relationele vermogen. Met dit vermogen is de politie in staat tot relatievorming en betekenisvolle ontmoetingen met burgers.

Opkomende technologieën kunnen de van oorsprong menselijke uitvoering van politiewerk versterken – het menselijke vermogen wordt dan vergroot – maar op onderdelen ook automatiseren. Van welke impact sprake is, hangt onder andere af van welke vermogens voor de taakuitvoering worden ingezet.

Ogen van de politie

Het surveillancevermogen wordt sterk beïnvloed door opkomende technologieën. De politie maakt in de eerste plaats gebruik van allerlei sensoren – vooral (slimme) camera's – waarmee de gang van zaken in de fysieke wereld wordt geobserveerd. Daarnaast worden uiteenlopende softwareprogramma's ingezet om online activiteiten van burgers te monitoren.[3] Het waarnemingsvermogen van de politie wordt door gebruik van deze technologieën exponentieel uitgebreid. Dit betreft niet alleen het vergroten van menselijke vermogens, maar ook het automatiseren of vervangen ervan. De chef van het real-time intelligence center van de eenheid Amsterdam gaf na de aanhouding van de verdachten van de moord op Peter R. de Vries het volgende aan: "Tien tot vijftien jaar geleden werden verdachten in soortgelijke situaties minder snel gepakt. Toen moesten de lokale eenheden op een viaduct boven de snelweg of op de vluchtstrook worden gepositioneerd om te zien of de verdachten voorbijkwamen."[4] Nu was het een ANPR-camera die de vluchtauto heeft waargenomen en eraan heeft bijgedragen dat de verdachten op de A4 bij Leidschendam door politieagenten konden worden klemgereden. Het voorbeeld van de aangehouden verdachten illustreert niet alleen dat sensoren worden gebruikt om menselijke activiteiten te automatiseren, maar laat ook zien wat de potentie van 'sensorsurveillance' is. De exponentiële uitbreiding van het waarnemingsvermogen van de politie biedt de mogelijkheid om criminaliteit beter te detecteren en op te sporen.[5] Deze medaille heeft echter ook een keerzijde. Door het combineren en analyseren van data uit verschillende sensoren en systemen neemt de diepgang van surveillance toe.[6] Dit kan leiden tot meer inbreuk op de privacy van burgers. Dit doet zich vooral voor bij burgers die niet worden verdacht van een strafbaar feit, maar wel als risico worden aangemerkt. Zij worden nader bekeken en mogelijk meer gecontroleerd.

> Voor het **relationele vermogen** van de politie zijn politiemensen nodig

Brein van de politie

Het cognitieve vermogen van de politie wordt ook – en misschien wel vooral – sterk beïnvloed door opkomende technologieën. Dit komt door het groeiend aantal algoritmen waarmee allerlei data in het kader van politietaken worden verwerkt. Deze algoritmen zijn onderdeel van softwareprogramma's die voor uiteenlopende doeleinden worden ingezet. Het betreft algoritmen die worden ingezet om gebeurtenissen die hebben plaatsgevonden te reconstrueren (terug), de gang van zaken in de samenleving te observeren (huidig) en criminaliteit te voorspellen (vooruit).[7] Algoritmen kunnen zowel door mensen zijn geprogrammeerd als zelflerend zijn op basis van data. In het laatste geval is er sprake van *machine*

1 Zie Wetenschappelijke Raad voor het Regeringsbeleid (2021). *Opgave AI. De nieuwe systeemtechnologie.* Den Haag: WRR.
2 Dit artikel is gebaseerd op een nog te publiceren boek getiteld *Politiewerk aan de horizon; technologie, criminaliteit en de toekomst van politiewerk.*
3 Zie Landman, W. & Groothuis, S. (2022). *Politiewerk op het web. Een verkennend onderzoek naar online gegevensvergaring door de politie.* Den Haag/Amersfoort: Politie & Wetenschap/Twynstra-Gudde.
4 Zie https://www.nrc.nl/nieuws/2021/07/16/hoe-verdachten-aanslag-peter-r-de-vries-zo-snel-konden-worden-gearresteerd-a4051328
5 Simmons, R. (2019). *Smart surveillance. How to interpret the fourth amendment in the twenty-first century.* Cambridge: Cambridge University Press.
6 Brayne, S. (2021). *Predict and surveil. Data, discretion, and the future of policing.* New York: Oxford University Press.
7 Zie ook Schuilenburg, M. & Sodijn, M. (2021). Big data in het veiligheidsdomein: Onderzoek naar big datatoepassingen bij de politie en de positieve effecten hiervan voor de politieorganisatie. *Tijdschrift voor veiligheid, 1,* 1-19.

> **Opkomende technologieën** (kunnen) zorgen voor een substantiële **uitbreiding** van het vermogen van de politie tot **waarnemen** en **informatie** verwerken

learning; de methode van artificiële intelligentie die op dit moment dominant is.
Door algoritmisering wordt het politiewerk niet meer beperkt tot de cognitieve vermogens van politiemensen. Dit is vooral van belang wanneer grote hoeveelheden gegevens moeten worden verwerkt, zoals onder andere het geval is bij het maken van veiligheidsbeelden en doen van voorspellingen op basis van uiteenlopende data of bij opsporing op basis van grote hoeveelheden cryptocommunicatiedata. Hierbij worden menselijke taken op onderdelen geautomatiseerd, maar blijft de politiemens een belangrijke rol spelen, onder andere omdat de uiteindelijke oordeels- en besluitvorming niet kan worden uitbesteed aan machines.

Tanden en hart van de politie

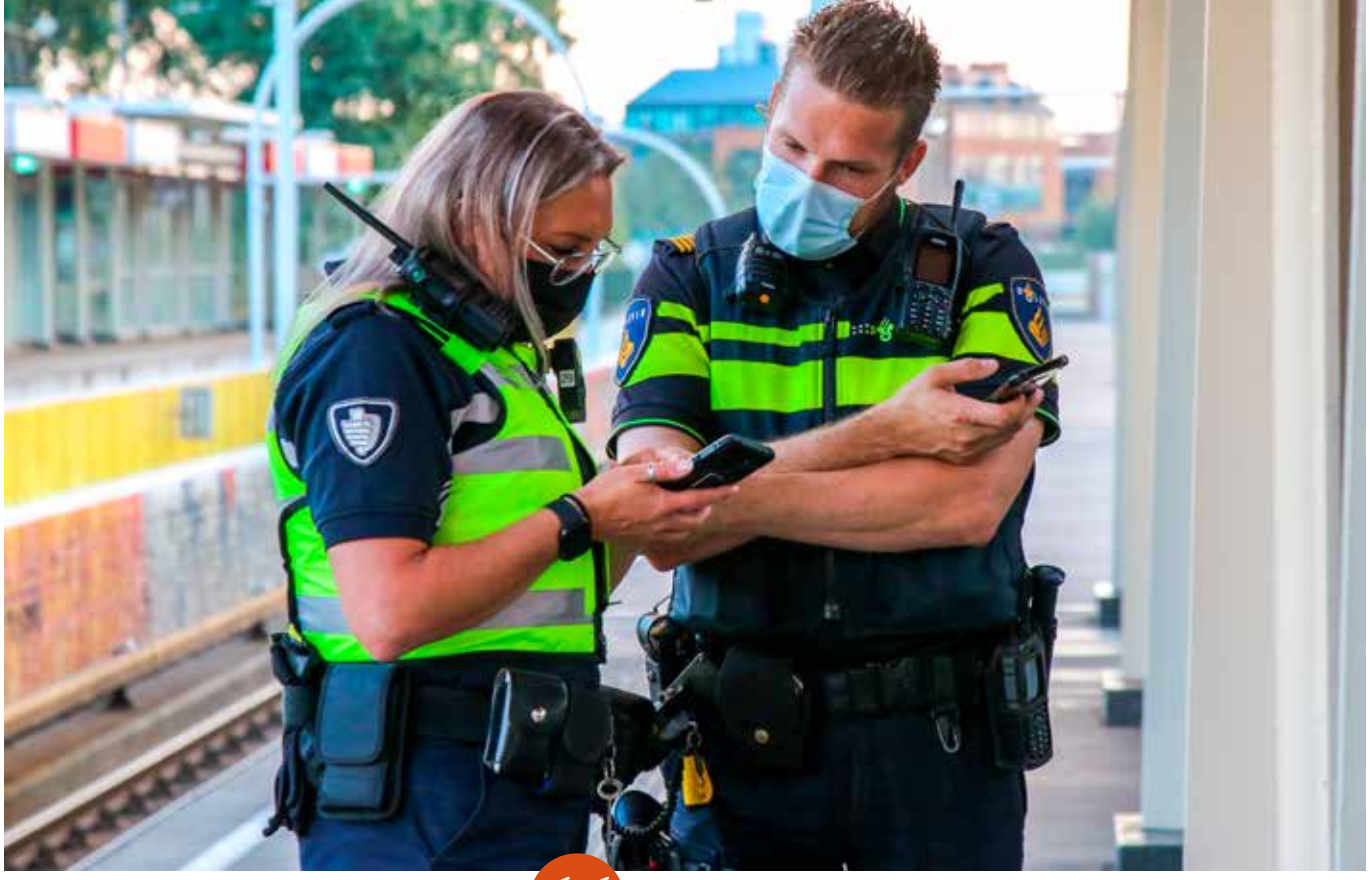
Technologische ontwikkelingen spelen ook een rol in het versterken van het fysieke vermogen van de politie. Zo is onlangs – op basis van een pilotperiode in twee basisteams – het stroomstootwapen aan de geweldsmiddelen van de politie toegevoegd. De opkomende technologieën van de vierde industriële revolutie hebben op de tanden van de politie echter (veel) minder invloed dan op de ogen en het brein van de politie. Hiervan zou wel sprake zijn als bijvoorbeeld robothonden met geweldsmiddelen worden uitgerust, maar hier is in Nederland geen sprake van. Toen robothond Spot voor het eerst werd ingezet voor het verkennen van explosiegevaar, is juist expliciet aangegeven dat van inzet in geweldsituaties dan wel uitrusting met geweldsmiddelen geen sprake zal zijn.

Dan het hart van de politie. Sherry Turkle, hoogleraar aan het Massachusetts Institute of Technology, onderzoekt al geruime tijd de impact van artificiële intelligentie op mensen. In haar memoires *The empathy diaries* betoogt ze dat AI systemen kunnen leren om te denken en te praten, maar niet om empathisch te zijn.[8] De kracht van empathie onderscheidt mensen van de slimme systemen die hen zo dicht weten te benaderen en op onderdelen ook overtreffen. Dit gegeven bepaalt volgens haar dat wij in het tijdperk van AI onze menselijkheid zullen behouden. En dit geldt ook voor politiemensen. Voor het relationele vermogen van de politie zijn politiemensen nodig. Vandaag, morgen en overmorgen.

Technologie in de kern

Op basis van het voorgaande is mijn stelling dat opkomende technologieën (kunnen) zorgen voor een substantiële uitbreiding van het vermogen van de politie tot waarnemen en informatie verwerken. Dit heeft als gevolg dat de relatie tussen technologie en politiewerk van karakter verandert. In de afgelopen decennia heeft technologie – het gaat dan in het bijzonder om informatie- en communicatietechnologie – het politiewerk vooral ondersteund. Zo kunnen politiemensen op straat via hun smartphone systemen raadplegen. De informatie die dit oplevert, kan van invloed zijn op hun betekenisgeving en daarmee op hun optreden. Dit doet zich bijvoorbeeld voor wanneer politiemensen een situatie als verdacht beschouwen en het natrekken van het voertuig tot antecedenten van de kentekenhouder leidt. Dan is er meer aanleiding om tot een proactieve controle over te gaan.[9]
Opkomende technologieën zorgen ervoor dat technologie zich beweegt van secundair naar meer primair. Anders gezegd: politiemachines worden invloedrijker in het primaire proces. Technologie voert processen uit die zich in de kern van het politiewerk bevinden. Het gaat dan vooral om processen van betekenisgeving, waaronder waarnemen van gebeurtenissen, verdacht gedrag identificeren en analyseren en redeneren. Neem als voorbeeld de inmiddels beëindigde proeftuin sensing in Roermond

8 Turkle, S. (2021). *The empathy diaries. A memoir.* New York: Penguin Press.
9 Zie Landman, W. & Kleijer-Kool, L. (2016). *Boeven vangen. Een onderzoek naar proactief politieoptreden.* Den Haag/Amersfoort: Politie & Wetenschap/Twynstra-Gudde.
10 Zie o.a. Stevens, L., Hirsch Ballin, M., Galič, M., Buisman, S.S., Groothoff, B., Hamelzky, Y., Lucas, C., Rasul, K. & Verijdt, S. (2021). Strafvorderlijke normering van preventief optreden op basis van datakoppeling Een analyse aan de hand van de casus 'Sensing-project Outlet Roermond'. *Tijdschrift voor Bijzonder Strafrecht & Handhaving, 4*, 234-245.
11 Zie o.a. Koper, C.S., & Lum, C. (2020). Technology in policing: critic. The limits of police technology. In: D. Weisburd & A.A. Braga (eds.), *Police innovation. Contrasting perspectives (2nd edition)*, Cambridge: Cambridge University Press, 517-543. Zie voor een voorbeeld van een onderzoek in Nederland: Mali, B., Bronkorst-Giesen, C. & Hengst, M. den (2017). *Predictive policing: lessen voor de toekomst. Een evaluatie van de landelijke pilot.* Apeldoorn: Politieacademie.



> **Vernieuwing** in politiewerk is een **samenspel** tussen **mensen** en **technologie** in een **organisatorische** context

ter bestrijding van mobiel banditisme.[10] In deze proeftuin is een sensornetwerk gebruikt dat vooral bestaat uit camera's met *automatic number plate recognition* (ANPR). De data die via sensoren worden verzameld, worden gecombineerd verwerkt en vergeleken met een profiel. Deze vergelijking leidt tot een risicoscore. Bij een hoge risicoscore wordt er een 'hit' doorgegeven aan dienstdoende agenten die vervolgens bepalen of zij het betreffende voertuig stilhouden en eventueel nader controleren. Dit voorbeeld illustreert hoe de rol van technologie langzamerhand verandert: processen van betekenisgeving *in* het politiewerk worden versterkt en op onderdelen geautomatiseerd.

Weerbarstigheid in technologie-adoptie

De (exponentiële) uitbreiding van het waarnemings- en cognitieve vermogen van de politie en de daarmee samenhangende veranderende rol van technologie hebben nog niet zomaar vernieuwing van politiewerk tot gevolg. Een rode draad in empirisch onderzoek naar technologie-adoptie in het politiewerk is dat het gebruik van nieuwe technologieën vaak wordt ingepast binnen de al bestaande manieren van werken.[11] Hierdoor wordt de potentie van technologie niet waargemaakt.

Ik geef enkele voorbeelden uit ons land die dit punt illustreren. *Predictive policing* brengt niet zomaar verandering in de wijze waarop en flexibiliteit waarmee capaciteit wordt gepland en in de manier waarop politieagenten surveilleren. Cryptodata leiden niet zomaar tot een meer probleemgerichte (systeem-) aanpak van georganiseerde criminaliteit. De beschikbaarheid van mobiele (DNA) identificatietechnologie leidt er niet zomaar toe dat de focus op het vinden van de verdachte – de *wie-heeft-het-gedaan-routine* – verandert in meer nadruk op de reconstructie van het misdrijf (*wat is er gebeurd?*). Kortom: technologische ontwikkelingen in het politiewerk bieden kansen op een andere manier van organiseren en werken, maar deze kansen worden niet vanzelf verzilverd.

> **Loskomen van** de bestaande **routines** en met verbeeldingskracht **nieuwe manieren** van werken realiseren

Technologie is niet deterministisch. Vernieuwing in politiewerk komt al dan niet tot stand in sociale praktijken. In een samenspel tussen mensen en technologie in een organisatorische context. Dit is aan de ene kant een zegen, want technologie gaat niet zomaar met het politiewerk 'aan de haal'. Het is aan de andere kant een vloek, want de adoptie van nieuwe technologie in het politiewerk is weerbarstig en dit maakt de uitkomsten enigszins onvoorspelbaar.[12] Deze weerbarstigheid wordt vooral veroorzaakt door de dominante manier waarop (uitvoerende) politiemensen naar politiewerk kijken en de doorwerking van deze manier van kijken op het gebruik van technologie.[13] Om het concreet te maken: als politiemensen het uitvoeren van strafrechtelijk onderzoek als de essentie van het werk zien, dan zullen zij ook op deze wijze naar het gebruik van technologie kijken. Dit beïnvloedt de manier waarop de technologie wordt gebruikt en daarmee ook de uitkomsten die dit gebruik heeft. Het risico bestaat dat dominante, decennialang bestaande, patronen in het politiewerk eerder worden versterkt dan doorbroken. Dit is een belemmering wanneer vernieuwing van politiewerk het streven is. En dit is bij de introductie van nieuwe technologieën geregeld het geval.

Technologische en sociale innovatie

Hoe om te gaan met deze weerbarstigheid? Een van de belangrijkste handelingsperspectieven is de combinatie van technologische en sociale innovatie. Vanaf de start van de technologieontwikkeling dienen de gewenste veranderingen in de manier van werken te worden meegenomen. Bijvoorbeeld: bij het ontwikkelen van een geavanceerd softwareprogramma voor het maken van veiligheidsbeelden is het essentieel dat er voldoende oog is voor de wijze waarop met deze beelden moet worden gestuurd en gewerkt. Anders is de kans te groot dat technologie wordt geïmplementeerd binnen een bestaande manier van werken en daarmee onvoldoende tot diens recht of potentie komt.

Onderzoek in het bedrijfsleven wijst uit dat de organisaties die hun werk opnieuw uitvinden – *re-imagine work* – het best in staat zijn om de potentie van opkomende technologieën te benutten.[14] Dit gaat (dus) ver voorbij het digitaliseren van bestaande werkprocessen. Kenmerkend voor de nieuwe werkprocessen is dat deze minder sequentieel zijn vormgegeven. Terug naar het voorbeeld: een veiligheidsbeeld is dan niet meer het begin van een keuzeproces in de opsporing, maar staat centraal in een cyclisch proces van een probleemgerichte aanpak waarvan ook allerlei niet strafrechtelijke interventies een onderdeel zijn. Een ander kenmerk is de samenwerking tussen mens en machine: mensen werken 'zij aan zij' samen met machines. Ervaringskennis van mensen interacteert en integreert met de machinale, statistische (algoritmische) manier van redeneren. Hierdoor ontstaat een vorm van hybride intelligentie.[15] Terug naar het voorbeeld: analisten maken gebruik van geavanceerde software voor het bewerken en analyseren van data en gebruiken hun ervaringskennis met betrekking tot criminele processen en subjecten om een uiteindelijk intelligenceproduct te maken.

De voornaamste uitdaging voor de politieorganisatie is om los te komen van de bestaande routines en met verbeeldingskracht nieuwe manieren van werken te realiseren. Alleen dan kan de potentie van de opkomende technologieën die zich nu aandienen ten volle worden benut. •

12 Zie Terpstra, J. & Salet, R. (2020). Big data policing als sociale praktijk. In J. Janssens, W. Broer, M. Crispel & R. Salet (Ed.), *Informatiegestuurde politie* (pp. 25-38). Turnhout/'s Hertogenbosch: Gompel&Svacina.

13 Zie o.a. Chan, J.B.L. (2003). Police and new technologies. In: T. Newburn (ed.). *Handbook of policing*, Cullompton: Willan, 655-679. En ook: Lum, C., Koper, C.S. & Willis, J. (2017). Understanding the limits of technology's impact on police effectiveness. *Police Quarterly*, 20(2), 135-136.

14 Daugherty, P.R. & Wilson, H.J. (2018). *Human + machine. Reimagining work in the age of AI*. Boston: Harvard Business Review Press.

15 Waardenburg, L. (2021). *Behind the scenes of artificial intelligence. Studying how organizations cope with machine learning in practice*. Haveka.

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 criminele fenomenen of op patronen die gerelateerd kunnen worden aan criminele gebeurtenissen in het verleden, bijvoorbeeld wapen- en drugshandel 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.

Tekst: Marc Schuilenburg & Martijn Wessels • Foto: Meesters Multi Media

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

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;

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/ldjusthom/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-guidelines-trustworthy-ai.

Algemene Rekenkamer, 2021). Toch moet hier worden gewaakt voor techno-triomfalisme. 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 wet op het gebied van data en privacy uit de koker van de Europese Unie.

> Neem **gebruikers** en **burgers** mee in de **ontwikkeling** van algoritmische toepassingen

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 Intellligence 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

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

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: Politieacademie.
- 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.

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. 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.

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

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.


College voor de Rechten van de Mens
Mensenrechten in Nederland 2021

“Er moeten **meer mogelijkheden** komen voor daadwerkelijke **rechtsbescherming**”

ONDERVOORZITTER EN COMMISSIELID BIJ HET COLLEGE VOOR DE RECHTEN VAN DE MENS

QUIRINE EIJKMAN

Barbara van Caem en Joery Matthys interviewden voor het themanummer ‘Politie in de informatiesamenleving’ Quirine Eijkman PhD. Als rechtssociologe kijkt zij naar hoe het recht in de praktijk wordt toegepast. De reden voor het interview is dat zij voor het College het strategisch programma digitalisering en mensenrechten trekt. Dat gaat niet specifiek over de politie, maar er zijn wel veel parallellen, denk maar aan risicoprofilering en etnisch profileren. Vanuit het lectoraat ‘Toegang tot het Recht’ aan het Kenniscentrum Sociale Innovatie (KSI) van Hogeschool Utrecht focust zij ook op digitale geletterdheid: er zijn behoorlijk wat laaggeletterde mensen in Nederland en dan kan het behoorlijk ingewikkeld zijn om met de politie te communiceren als die voluit de digitale kaart trekt. We spraken met Quirine Eijkman in haar woonkamer midden in Amsterdam.

Tekst: Joery Matthys & Barbara van Caem • Foto’s: Erik Laan Photoos, Haarlem

> “Ik vind dat de mensen die die systemen aanschaffen een **verantwoordings-plicht** hebben”

Dit nummer van het *Tijdschrift voor de Politie* gaat over de informatiesamenleving en we denken daarbij aan twee belangrijke thema’s, namelijk dataverzameling door de politie enerzijds en de rol die de politie kan spelen in het tegengaan van desinformatie anderzijds. Beide thema’s kunnen sterk gelinkt worden aan mensenrechten. Laten we ons eerst concentreren op dataverzameling, de informatiepositie van de politie. Wat zijn de potentiële conflicten met mensenrechten?

De hele discussie over *intelligence led policing* is natuurlijk niet nieuw; de politie die gebruikmaakt van de eigen informatiepositie om haar taken uit te voeren, dat is eigenlijk gewoon goed politiewerk. Maar het wordt problematisch wanneer heel veel autoriteit wordt toebedeeld aan voorspellende systemen, die trouwens zeker niet alleen door de politie gebruikt worden. Er zijn twee grote problemen, die ook gelinkt zijn aan elkaar: de mogelijkheid van discriminatie en dirty data. Zo gaf ik een keer gastcollege aan een groep studenten uit Delft, waarvan veel een migratieachtergrond hadden, en we hadden het over preventief fouilleren. Als de studenten met een migratieachtergrond dan vertelden dat ze elk jaar wel vijftien keer gecontroleerd worden door de politie, terwijl het gewoon niet gebeurde bij de aanwezige witte mensen, dan doet dat iets met je op menselijk vlak, maar ook als wetenschapper moet je je de vraag stellen: wordt dit geen self-fulfilling prophecy, waarbij gegevens verzameld op basis van discriminatie een systeem voeden dat op zijn beurt die discriminatie gaat valideren? De toeslagenaffaire is natuurlijk hét voorbeeld van zo’n vicieuze cirkel, waarbij er ook geen kritische vragen meer gesteld worden door de gebruikers van het systeem. Vanuit het College van de Rechten van de Mens willen we natuurlijk dat iedereen in Nederland gelijk behandeld wordt, dus dit is voor ons een belangrijk aandachtspunt. Dat betekent ook niet dat we per definitie tegen het gebruik van die systemen zijn, maar wij vinden dat er transparantie moet zijn, en een kritische houding. De politie moeten zich de vraag stellen of die systemen en/of de informatie die daaruit voortkomt wel klopt. En dat blijkt heel ingewikkeld, er is nog heel veel onduidelijk, en het is een lastig intern gesprek waarschijnlijk ook bij de politie.

Is de kwaliteit van de politiegegevens dan zo problematisch in Nederland?

Dat is het punt, het is heel moeilijk om dat te evalueren. Ik vind dat de politie het heel goed uitlegt, maar de insteek onder andere over het Criminaliteits Anticipatie Systeem (CAS) is erg vanuit de ‘communicatie’. Het helpt ons, we kunnen onze middelen hierdoor meer doelmatig inzetten, etc. Voor mij gaat het over accountability, en dat moet op verschillende niveaus gebeuren. Ik ben copromotor van het onderzoek van Daan Weggemans, en dat gaat gedeeltelijk om de vraag of uitvoerende professionals zoals de agenten op straat voldoende in staat zijn om terug te koppelen over hun ervaringen met dit soort systemen, en wat er gebeurt met die feedbackloop. Ik vind dat de mensen die die systemen aanschaffen een verantwoordingsplicht hebben, dat zij het systeem zo moeten inrichten dat het toetsbaar is voor eindgebruikers. Want dit soort systemen worden steeds meer ontwikkeld en gebruikt. Ethische hackers vertellen mij dat de mensen die verantwoordelijk zijn voor hun gebruik, eigenlijk niet goed snappen hoe ze precies werken. Dus niemand klaagt over het gebruik

Over de auteurs
Joery Matthys is universitair docent aan het Institute of Security and Global Affairs (Universiteit Leiden). Dr. mr. Barbara van Caem is hoofd van de cluster wetenschap bij de Landelijke Portefeuille Gebiedsgebonden Politie.

van die systemen, terwijl mijn eigen onderzoek naar vroegsignalering op radicalisering en extremisme al twijfels plaatste bij de mogelijkheden om hierover voorspellingen te maken. Dat lukt voor bepaalde types criminaliteit, maar vaak is het toch niet zo duidelijk. Ik vraag me ook af in hoeverre kritisch gebruik van algoritmen wordt meegenomen in de opleiding van agenten. De technologie laat de voorspellingen die algoritmen doen objectief en neutraal lijken, en daar zit net het gevaar. Van belang is ook je te realiseren wat het doet met mensen om op zulke lijsten te komen. Ik heb de vrije val gezien waar mensen in terechtkomen die door de toeslagenaffaire werden getroffen. Daar zie je de macht van de informatie en wat de overheid de burger daarmee aan kan doen. Er moeten meer mogelijkheden komen voor daadwerkelijke rechtsbescherming.

Dat is een belangrijke bedenking en waarschuwing. Maar gaan er ook dingen goed in Nederland?

Ik vind het heel positief dat de discussie op gang is gekomen en dat de kennis van beleidsmakers en leidinggevenden wel is toegenomen. Ondanks die eerdere waarschuwing, ben ik eigenlijk best positief. Er zijn heel veel gesprekken hoe dat kan, er worden nieuwe tools ontwikkeld. Ook de discussie over etnisch profileren is op gang gekomen, zeker sinds Amnesty International en Control Alt Delete[1] dit hebben aangekaart. Belangrijk is hierbij dat de politie blijft engageren en zich laat adviseren door 'buitenstaanders'. Wie bij de politie begint te werken is al snel blauw gekleurd, one of us. En dan kan je de aansluiting kwijtraken, je kan uit het oog verliezen wat er speelt buiten het directe gezichtsveld. Dat besef is echt wel meer aanwezig bij de politie, dat is een zeer positieve ontwikkeling geweest. Natuurlijk, voeg de daad bij het woord, het moet ook uiteindelijk tot iets leiden. De mechanismen moeten nog aangepast worden. Er zijn bijvoorbeeld nog veel mensen die zich gediscrimineerd voelen, terwijl ze tegelijkertijd nauwelijks klagen of aangifte doen bij de politie. Dit komt enkel naar boven bij surveys. Maar het doet wel iets met de legitimiteit van een zeer belangrijke organisatie in Nederland. Dus je hebt 'buitenstaanders' nodig, en je moet de interne mensen die kritische vragen stellen, ook koesteren. Want die zijn er ook echt wel, dat is ook weer positief. Veel mensen binnen de politie houden van hun vak en willen het beter maken. Natuurlijk, daar zitten we ook weer met het probleem dat wanneer we het over voorspellende systemen hebben, er weinig mensen zijn die het systeem echt snappen. En diegenen die het wel snappen, hebben niet steeds invloed op het beleid rond deze systemen.

Toetsingskader discriminatie risicoprofielen

Wordt er een onderscheid gemaakt in het risicoprofiel op basis van ras of nationaliteit?

- Leidt de inzet van het risicoprofiel tot een ongelijke behandeling op grond van ras of nationaliteit?
- Is de ongelijke behandeling ook te herleiden naar ras of nationaliteit, of spelen er andere factoren?

Is er een mogelijke rechtvaardiging om een onderscheid te maken op basis van ras of nationaliteit?

- Wordt een legitiem doel nagestreefd?
- Is er sprake van evenredigheid tussen het nagestreefde legitieme doel en het inzetten van een risicoprofiel dat een onderscheid maakt op basis van ras of nationaliteit?
- Is er beoordelingsruimte om deze afweging te maken?

> “Als je op je **achttiende** een stommiteit hebt uitgehaald, **hoelang** moet je dat dan **meeslepen**?”

Hoe verhoudt Nederland zich tegenover andere landen hierin?
Wel, Nederland is met digitalisering echt wel heel hard gegaan en staat dus vaak voorop. Maar door deze snelheid heeft het zich initieel ook, laten we zeggen, ‘pragmatisch’ opgesteld. Eerst gewoon doen en dan achteraf bedenken hoe grondrechten en mensenrechten van belang kunnen zijn. Het feit dat die reflectie er komt, is natuurlijk een stap in de goede richting. Maar Nederland ziet zichzelf toch als ‘mensenrechtengidsland’, en dan is het toch wel nodig dat het besef er is dat dit ook geldt voor onze eigen burgers. Dan gaat het niet enkel over privacy, het gaat ook om gelijkheid, om toegang tot het recht, etc.

Het College voor de Rechten van de Mens is niet alleen toezichthouder, maar tracht ook wetgeving en het beleid met mensenrechten rekening te laten houden. Wat zijn de handvatten die jij zou aanreiken om een systeem op te zetten dat rekening houdt met de issues die we hiervoor besproken hebben?
Wel, we hebben het al over transparantie gehad, natuurlijk, dat is één. Het College heeft ook een mensenrechtelijk toetsingskader[2] ontwikkeld om discriminatie door risicoprofielen tegen te gaan. Daar staan een aantal handvatten in om het systeem echt te verbeteren. We hebben gemerkt dat er veel gaande is, ook op Europees niveau, maar het moet ook gebruikt worden. Dat was het doel van het toetsingskader, om het in de Nederlandse context ook om te zetten, vanuit onze rol als hoeder van mensenrechten.
Daarnaast moet er ook voldoende besef zijn bij de politie hoeveel macht informatie geeft. Ik gaf een tijd geleden een gastles over accountability. Ik noemde daarbij als voorbeeld dat iemand verdacht werd van fraude, waardoor de laptop van die persoon werd doorgenomen. Dan kan je echt wel andere informatie vinden, die je als politie ook mogelijk kan gebruiken tegen die persoon, bijvoorbeeld om een bekentenis af te dwingen. Daar moet voorzichtig mee omgegaan worden, die macht moet begrepen worden. Zeker als ook nog eens blijkt dat de informatie foutief was, maar toch als instrument ingezet wordt. Dat doet me denken aan een rapport van de Ombudsman[3], over een Nederlands Surinaamse zakenman wiens klasgenoot verslaafd was maar die telkens wanneer hij aangehouden werd de naam opgaf van eerstgenoemde. Dat was schrijnend, en werd verzwaard door de uitwisseling van gegevens tussen publieke diensten. Die man werd telkens staande gehouden, kon geen leningen meer krijgen, kon de Verenigde Staten niet meer binnen, etc. De politie zelf wist wel wat er gaande was, maar de systemen konden simpelweg niet gecorrigeerd worden. Iedereen was verantwoordelijk voor het bijhouden van de informatie, dus niemand voelde zich verantwoordelijk, dat is het probleem van het gebrek aan eigenaarschap. Dus die mogelijkheid tot correctie naar aanleiding van identiteitsfraude, dat is toch ook belangrijk. Informatie is macht, zeker informatie die zeer lang bewaard wordt. Als je op je achttiende een stommiteit hebt uitgehaald, hoelang moet je dat dan meeslepen?

Als laatste vraag willen we het ook over desinformatie hebben en de mogelijke rol die politie hierin kan spelen. Dat leunt natuurlijk aan bij het recht op vrije meningsuiting en het mogelijke gevaar dat bestrijding van desinformatie op een bepaald moment *policing the truth* wordt, wat evenzeer ongewenst is. Wat is volgens jou de rol die de politie kan of moet spelen?
Wat desinformatie betreft, kan ik ten volle de jaarrapportage van het College[4] aanraden, omdat die daar toch een belangrijk deel aan wijdt. Desinformatie treft niet alleen de politie maar vooral ook de politiek. De politie

1 https://controlealtdelete.nl/
2 https://open.overheid.nl/repository/ronl-c409ea31-2c00-4318-9a45-d47ad8a2ca7f/1/pdf/crm-discriminatie-door-risicoprofielen-mensenrechtelijk-toetsingskader.pdf
3 https://www.nationaleombudsman.nl/nieuws/2009/ombudsman-biedt-bemiddeling-aan-bij-identiteitsfraudezaak
4 https://publicaties.mensenrechten.nl/file/99134603-807b-4eaa-95a0-b93a78fda248.pdf
5 Doxing is de handeling waarbij identificerende informatie over iemand online wordt onthuld, zoals zijn of haar echte naam, woonadres, werkplek, telefoon, financiële en andere persoonlijke informatie. Die informatie wordt dan openbaar gemaakt zonder toestemming van het slachtoffer.

heeft daar ook een rol te spelen, al was het maar enkel om diegenen op te sporen die journalisten of experts lastig vallen. Zelf ben ik het scherpst op intimidatie, denk aan het online openbaar maken van identificeerbare informatie of doxing[5]. Dat zijn best wel reële problemen die sterk gelinkt zijn aan de vrijheid van meningsuiting. We vinden dat belangrijk. Maar de jaarrapportage bedeelt toch ook een belangrijke rol aan de overheid en platformbedrijven, deze hebben een zorgplicht hierin. Dat betekent niet dat de politie dan een stap opzij moet zetten. Zij heeft de mogelijkheid om in te stappen, aan te kaarten, te corrigeren. Dan gaat het om de tegenboodschap. De politie is daar niet altijd de meest geschikte organisatie voor, maar vaak ook wel. Ze kunnen snel reageren. Er was onlangs een jongen die mogelijk ontvoerd was, en op sociale media werd een verdachte aangeduid. De politie heeft daar heel snel op gereageerd en heeft duidelijk gemaakt dat deze persoon niet de verdachte was. Dat was belangrijk om te doen, je krijgt al snel een – online – heksenjacht. Je leven is snel kapot gemaakt als

> “Er zijn veel mensen die zich **gediscrimineerd** voelen, terwijl ze tegelijkertijd **nauwelijks klagen** of **aangifte** doen bij de politie”

je in verband wordt gebracht met criminele feiten, zeker als er bijvoorbeeld een seksueel element of een element met een minderjarige aan vasthangt. De politie kan door een snelle reactie heel veel problemen voorkomen. Over zowel dataverzameling door de politie als desinformatie zouden we eigenlijk nog uren kunnen doorpraten, maar ik wil vooral nog een laatste punt benadrukken: deze problematiek raakt niet alleen de politie, maar ook andere uitvoeringsorganisaties. Net zoals de problemen gezamenlijk zijn, moet er ook samen tot oplossingen gekomen worden. •

Verder lezen op de website

Op www.websitevoordepolitie.nl worden geregeld artikelen geplaatst die cirkelen rond het thema van een themanummer of artikelen die anderszins passen in het beleid van de redactie. De website biedt de mogelijkheid om te reageren op de artikelen en om via de beschikbare social media het artikel onder de aandacht van anderen te brengen.

De volgende artikelen sluiten aan bij het thema 'Informatiesamenleving'. We introduceren ze kort. Op de website zijn de integrale artikelen te lezen.

Invoering van het stroomstootwapen bij de Nederlandse politie

Vanaf 1 januari 2022 is het stroomstootwapen ingevoerd als nieuw geweldsmiddel in de basispolitiezorg. De meningen over het stroomstootwapen lopen nog steeds uiteen. Veel politiemensen zien het als een geweldig middel dat het mogelijk maakt om, vergeleken met andere geweldsmiddelen, gevaarlijke of gewelddadige personen met minder nadelige gevolgen voor hen en voor optredende agenten onder controle te brengen. Om die reden maken politiediensten in steeds meer landen gebruik van stroomstootwapens. Otto Adang, Bas Mali en Kim Vermeulen zetten de feiten rond het stroomstootwapen op grond van de evaluatie van de pilot op een rij. Bij juist gebruik tegen gezonde personen is gebruik van het stroomstootwapen niet gevaarlijk. Tegelijkertijd blijft het stroomstootwapen een ingrijpend geweldsmiddel, dat veel pijn veroorzaakt en personen enkele seconden lang de controle over hun lichaam laat verliezen waarbij er risico's zijn bij gebruik tegen verschillende groepen kwetsbare personen. Dat maant tot terughoudendheid in het gebruik. Lees het artikel verder via de QR-code.

De meningen over het stroomstootwapen lopen nog steeds uiteen

Slachtoffers van partnergeweld over strafrechtelijke verboden

Slachtoffers van partnergeweld hebben vaak behoefte aan bescherming. Eén van de middelen om slachtoffers te beschermen is een strafrechtelijk contact-, locatie of gebiedsverbod. Uit onderzoek blijkt dat iets meer dan de helft van de ondervraagde slachtoffers (van allerlei misdrijven) zich veiliger voelt door oplegging van zo'n verbod. Een minderheid voelt zich echter onveiliger. Het is onduidelijk hoe verboden hieraan bijdragen en de gevolgen hiervan voor hun dagelijks leven. Hierover ontbreekt zowel theoretisch als praktijkgericht onderzoek. Irma Cleven werkt aan een promotieonderzoek hierover. Hiermee hoopt zij inzicht te bieden in en aanknopingspunten te geven voor de verbetering van ondersteuning aan slachtoffers.

Iets meer dan de helft van de slachtoffers voelt zich veiliger door oplegging van een verbod

Trialoog over kennismanagement en digitale fitheid

Ze zijn alle drie binnen hun vakgebied actief bezig met kennisontwikkeling en de rol van kenniswerk binnen de politie. Techfilosoof Martijn Aslander schreef een boek over kenniswerk (*Ons werk is stuk!*), Teun Meurs schreef een proefschrift over kenniswerkers (*Tussen de linies*) en Teun-Pieter de Snoo werkt voor Kenniscentrum Mens & Politieorganisatie. Ze zijn het over één ding roerend eens: kennismanagement is een urgent en onderbelicht vraagstuk in de politie. Natuurlijk is het slim om als politie in de informatiesamenleving je kennis goed te ordenen en vast te leggen, zodat je die altijd snel kunt vinden en waar nodig kunt delen. Maar dat is maar één deel van het 'kennisverhaal' van de politie. Wat is kennismanagement en hoe doe je dat? Hierover gingen de drie onderzoekende collega's met elkaar in gesprek. Het verslag van deze verkennende en inspirerende trialoog is via de QR-code te downloaden.

Kennismanagement is een urgent en onderbelicht vraagstuk in de politie

Een beschouwing vanuit de hoofdportefeuille Kennismanagement

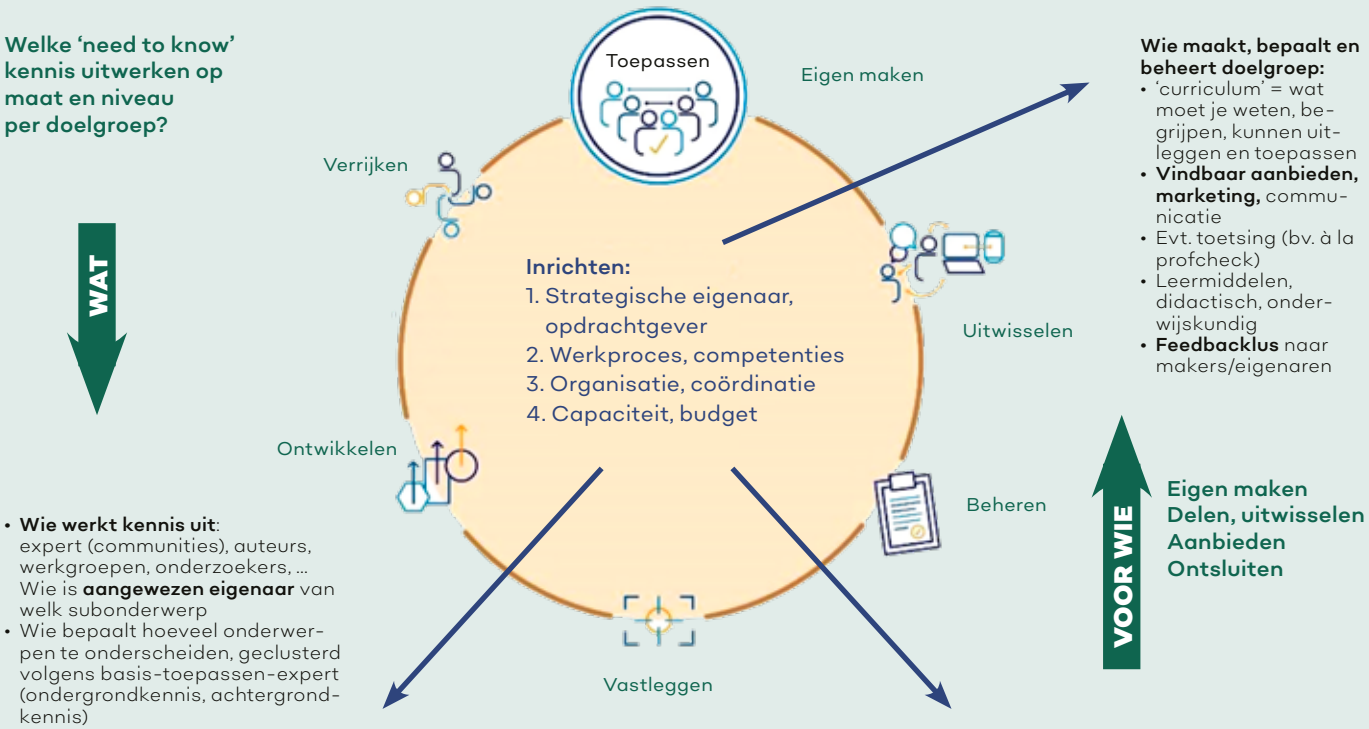
Het werkveld van de politie verandert in een snel tempo door een toenemend complexe samenleving met een stijgend belang van snelle technologische ontwikkelingen. Van de politieorganisatie wordt verlangd, zo niet geëist, in te spelen op deze veranderingen. Dit vraagt flexibiliteit en wendbaarheid van onze medewerkers op alle niveaus en een verdere professionalisering van het politievak, waarbij processen van het creëren, delen, gebruiken en beheren van kennis essentieel zijn.
Daarnaast versterkt de invoering van nieuwe en/of veranderende wetgeving, zoals het Wetboek van Strafvordering, de druk om kennis goed vast te leggen, eenvoudig te ontsluiten en vindbaar te maken voor alle medewerkers om foutief handelen te voorkomen. Ook wordt het steeds belangrijker om ervaringsdeskundigheid prominenter door te laten werken en dus vindbaarder te maken in de systemen.

Werk aan de winkel

Om in de huidige informatiesamenleving 'slimmer omgaan met onze kennis' te realiseren, is voortdurende aandacht voor het optimaliseren van de beschikbaarheid en het gebruik van kennis en informatie een must. Belangrijke vragen 'van alledag' zijn beknopt samengevat in onderstaande figuur.

Het volledige artikel **'Samen sterk door kennismanagement'** kan je lezen door de QR-code te scannen.

Over de auteurs
Rob Kouwenhoven en Sanne Visser MSc/MCI/CBP zijn strategisch adviseur kennismanagement bij de Directie Operatiën (staf korpsleiding).



Dr. Peter Klerks
Docent aan de Politieacademie en Raadsadviseur Parket-Generaal, Openbaar Ministerie

Bezielde techniek

Sciencefictionschrijver Arthur C. Clarke schreef in 1962: "Any sufficiently advanced technology is indistinguishable from magic." Wie zestig jaar later de mogelijkheden van geavanceerde opsporingsmethoden ervaart, raakt allicht gefascineerd. Data-analisten vissen feilloos relevante passages uit bijna een miljard versleutelde berichten. Forensisch onderzoekers lossen moordzaken op met microscopische sporen. Drones maken het mogelijk bij crisissituaties in real-time mee te kijken. Technici plaatsen afluistermicrofoons in zwaar beveiligde panden van drugshandelaren.

Krachtige techniek inzetten voor misdaadbestrijding wekt enthousiasme, maar brengt ook verantwoordelijkheid met zich mee. Onze rechtsstaat heeft niet als eerste opgave om boeven te vangen, maar burgers te beschermen tegen een almachtige overheid. Dat klinkt zwaar, maar wie beseft hoe ver instanties in de persoonlijke levenssfeer doordringen en inbreken op grondrechten, weet dat rechtsstatelijke bescherming geen overbodige luxe is. Bevoegdheidsoverschrijdingen bij de NCTV en inlichtingendiensten maakten dat recent weer duidelijk. Natuurlijk gebruiken politiemensen en OM'ers hun bevoegdheden niet naar willekeur. Ze vervullen hun ambtelijke plicht in het belang van de samenleving en leggen daarover doorgaans verantwoording af. Het blijft echter mensenwerk. Incompetentie, vooroordelen, gemakzucht en gebrekkige controle zijn maar enkele redenen waarom het soms toch uit de hand loopt.

Het kabinet gaf na aanhoudende onthullingen toe dat de inzet van geautomatiseerde profielen bij de Belastingdienst tot grote misstanden leidde, veroorzaakt door institutioneel racisme. In de rechtszaal bleek herhaaldelijk dat een ambtsedig opgemaakt relaas niet per definitie de waarheid weergeeft. Ook hardnekkige weerstand tegen diversiteit in de 'blauwe familie' leidde tot onrecht. Vrouwelijke collega's, mensen van kleur en anderen die van de traditionele norm afwijken betaalden daar een hoge prijs voor. Sommigen vonden de moed hun pijnlijke ervaringen met de buitenwereld te delen. Anderen vertrokken of proberen niet op te vallen. Enkelen pleegden zelfmoord. Voor hen bleek de politie een wezenlijk onveilige organisatie met falend moreel leiderschap.

> Met **controle** op opsporingsmethoden, dataopslag en algoritmen kunnen burgers hun overheid weer **vertrouwen**

Uit de wetenschap klinkt scepsis over zelfregulerend ethisch besef in opsporings- en inlichtingenwerk.[1] Ik kwam echter weinig cynische fanatici tegen die maximaal informatie willen binnenharken zonder over proportionaliteit en waarborgen na te denken. Sommige politiemanagers zijn verontrustend enthousiast over de film *Minority Report*, waarin Tom Cruise met techno-magie misdrijven oplost voordat die worden gepleegd. Daartegenover staan echter vele zorgvuldige gesprekken met rechercheurs, inlichtingenmensen en OM'ers op alle niveaus. Professionele collega's die ziel en zaligheid in hun werk leggen. Daarbij liepen afwegingen uiteen en waren er rekkelijken en preciezen. Er werd geklaagd over beperkende wetgeving en administratieve verantwoordingsdruk. Maar veel collega's beseffen terdege dat wie met zwaar geschut zoals kunstmatige intelligentie en hacks werkt, zich om schadebeperking moet bekommeren. Als medewerkers, leidinggevenden en de organisatie professioneel ethisch besef demonstreren en zich openstellen voor controle op opsporingsmethoden, dataopslag en algoritmen, kunnen burgers hun overheid weer vertrouwen. •

1 Onder meer K.V. Rønn (2018). The professional ethics of intelligence. On the feasibility of ethics as internal self-regulation of intelligence activities. Pp. 121-139 in: N. Fyfe, H. Gundhus & K.V. Rønn (Eds.). *Moral issues in intelligence-led policing*. London; New York: Routledge.

→ Reageren? p.p.h.m.klerks@om.nl

Technologie en de politie van de toekomst

EXPERIMENTEREN MET EN OPSCHALEN VAN KANSRIJKE TECHNOLOGISCHE INNOVATIES

Voor de politie is het om verschillende redenen van belang om in te spelen op technologische ontwikkelingen. Enerzijds moet de politie rekening houden met de impact van technologie op de maatschappij en de wijze waarop burgers, criminelen of terroristen gebruik maken van technologie. Anderzijds biedt technologie ook kansen om het politiewerk of de organisatie te verbeteren, versnellen of vergemakkelijken. Het team Science en Technology van de politie houdt bij welke technologieën en toepassingen een impact hebben op deze verschillende aspecten van het werk van de politie.

In de afgelopen jaren hebben technologische ontwikkelingen reeds merkbare gevolgen gehad voor het politiewerk, zoals de maatschappelijke gevolgen van social media en een verschuiving van criminaliteit naar het digitale domein. Cybercrime is veelal lucratiever dan 'traditionele criminaliteit' doordat snel schaalvoordelen kunnen worden behaald, de buit veel hoger is en de pakkans relatief lager is. Ook heeft technologie criminelen nieuwe tools geboden om criminaliteit uit te voeren, zoals het dark web en cryptocurrencies. De ontwikkeling van kunstmatige intelligentie biedt criminelen ook nieuwe mogelijkheden, bijvoorbeeld het inzetten van deepfakes om fraude te plegen. Verder maken technologische toepassingen als minicamera's, locatiesensoren, gezichtsherkenningsalgoritmes en domotica steeds verdergaande privacyschendingen mogelijk. Kwaadwillenden kunnen daarmee steeds gemakkelijker op allerlei manieren data, informatie en beelden verzamelen (of zelfs manipuleren) om anderen te stalken, te bespioneren, te chanteren of te bedreigen. Maar nieuwe technologieën bieden ook nieuwe doelwitten voor criminelen. Bijvoorbeeld het stelen van cryptocurrencies, NFT's of e-bikes. En er ontstaan nieuwe domeinen om criminaliteit te plegen, bijvoorbeeld straks in de metaverse. Met 3D-printing kunnen wapens worden geprint of in de toekomst wellicht designer drugs worden geproduceerd. Ook ontstaan nieuwe vraagstukken, bijvoorbeeld over de regulering van kinderseksrobots, waarover onlangs een WODC-rapport verscheen. In de verdere toekomst ontstaan wellicht ook nieuwe vraagstukken, bijvoorbeeld omtrent het tegen iemands wil gebruiken van DNA-materiaal voor genetische manipulatie.

Criminaliteitsbestrijding met technologie

Technologie biedt ook mogelijkheden om criminaliteit te voorkomen of beter te bestrijden. Camera's, domotica en locatiesensoren zorgen ervoor dat inbraak en diefstal niet zo snel meer ongemerkt gepleegd kunnen worden.

Over de auteur
M. Luursema werkt bij Team Science en Technologie van de Directie Strategie en Innovatie bij de Staf Korpsleiding. De afdeling Science en Technologie van de Directie Strategie en Innovatie bij de Staf Korpsleiding signaleert, monitort, analyseert en duidt technologische ontwikkelingen. De afdeling coördineert technologie-onderzoek en kennis, draagt bij aan het verhogen van expertise en kennis hierover, ontwikkelt visie, adviseert en zorgt voor het (laten) realiseren van aanpakken op relevante (veelal dwarsdoorsnijdende) thema's. Producten van het team zijn bijvoorbeeld de Science & Technology Agenda voor de Politie, de Technologiescan Politie en de tweewekelijkse Tech Gym-lezingen, de Tech Gym nieuwsbrief en het Innovatieportaal voor alle politiecollega's. Het Team is te vinden via innovatie@politie.nl of via intranet.

Tekst: M. Luursema • Fotos: Unsplash & Pexels

De **ontwikkeling** van **kunstmatige intelligentie** biedt **criminelen** nieuwe **mogelijkheden**

Er zijn zelfs experimenten uitgevoerd om met sensoren in een smart city een inbraakvrije wijk te creëren. Maar ook toepassingen als virtual reality worden ingezet om recidive bij daders tegen te gaan of slachtofferschap bij kwetsbare groepen te voorkomen. Cybersecurity kan worden verbeterd met behulp van kunstmatige intelligentie, door middel van 'automated vulnerability research'. Verder is het in principe mogelijk om met behulp van blockchaintechnologie fraudebestendiger distributiemechanismes te creëren, om bijvoorbeeld ticketfraude tegen te gaan.

Nieuwe veiligheidsdreigingen

Helaas zijn er nogal wat nieuwe technologieën die een potentiële dreiging voor de nationale veiligheid of zelfs de globale veiligheid vormen. Ze kunnen onvoorspelbare gevolgen hebben, wellicht zelfs onbeheersbare of onomkeerbare gevolgen die zich op grote schaal kunnen voordoen. In de discussie over klimaatverandering gaan er hier en daar stemmen op om te komen tot 'solar geo-engineering'. Minuscule deeltjes in de stratosfeer zouden zonlicht kunnen weerkaatsten, waardoor de aarde kunstmatig afkoelt en klimaatdoelen kunnen worden behaald. Anderen waarschuwen voor de onvoorzienbare gevolgen en mogelijke onbedoelde effecten voor flora en fauna. Een ander punt van zorg is de onvoorspelbaarheid van de ontwikkeling van steeds intelligenter wordende kunstmatige intelligentie (door sommigen ook wel 'the biggest threat to mankind' genoemd). Als kunstmatige intelligentie slimmer wordt dan de mens, kunnen we het dan nog wel beheersen? Maar ook op het gebied van life sciences ontstaan nieuwe risico's. Technieken die genetische manipulatie van mensen, planten, dieren en organismen mogelijk maken, worden veelzijdiger, eenvoudiger, goedkoper en komen op korte termijn veel breder beschikbaar, ook voor niet-wetenschappers. De toepassing van genome editing of synthetische biologie kan niet alleen leiden tot onbedoelde negatieve effecten; de technieken kunnen ook opzettelijk worden misbruikt. Een potentieel ernstig veiligheidsrisico hierbij op de middellange termijn is bioterrorisme en/of biowarfare, waarbij kwaadwillenden via een combinatie van synthetische biologie, bio-informatica en do-it-yourself biology custom-made (nieuwe) giftige stoffen en besmettelijke ziekten kunnen ontwikkelen. Ook nanotechnologie en verspreiding van nanodeeltjes in het leefmilieu kunnen ongekende en grote gevolgen hebben voor de natuur of de gezondheid. Digitale ontwikkelingen als 5G, cloud, quantum computing, satellieten, internet of things, smart grids, robotics, unmanned systems en zelfrijdende auto's zullen tot nieuwe afhankelijkheden leiden, en daarmee ook tot nieuwe kwetsbaarheden. Aan (cyber)security by design (nadenken over veiligheid aan de voorkant) wordt nog niet altijd voldoende aandacht besteed. Het kraken van beveiligingssleutels met behulp van kwantumtechnologie vormt al op termijn een groot risico voor cybersecurity en de vertrouwelijkheid van informatie, waar nu al actie voor nodig is. Technologieën als 3D-printing, unmanned systems, jetsuits, nanotechnologie, robotisering en kunstmatige intelligentie zijn straks – of soms nu al – voor iedereen op de markt verkrijgbaar en kunnen potentieel worden gebruikt als nieuwe modus operandi door kwaadwillenden c.q. terroristen. Unmanned systems kunnen bijvoorbeeld worden gebruikt om explosieven te transporteren. Daarnaast kan technologie op zichzelf ook een onderwerp vormen voor wantrouwen, polarisatie en zelfs extremisme. Zo leven er bij sommige groepen in de samenleving hevige ideeën over bijvoorbeeld 5G, robotica, nanotechnologie, life sciences, digitaal geld of identiteitssystemen.

Nieuwe manieren om veiligheid te vergroten

Technologische toepassingen kunnen worden ingezet om veiligheid te vergroten. Zo kunnen drones, onderwaterdrones, robots, jetsuits, satellieten en sensoren worden ingezet voor crisisbeheersing, search and rescue of brandbestrijding. Slimme camera's, sensoren, smart cities, drones, biometrie en apps kunnen ook worden ingezet voor crowd management, bewaken en beveiligen of toegangscontrole. Digital twins, smart cities en sensor-en-data-integratie kunnen zorgen voor een betere situational awareness. Tegelijkertijd spelen daarbij vraagstukken van proportionaliteit, grondrechten en ethiek. Dergelijke technologieën kunnen namelijk ook worden ingezet om de bevolking en mensenrechten te onderdrukken. In sommige landen gebeurt dit al feitelijk. Het efficiënter maken van het beveiligen van de samenleving kan – ook met goede bedoelingen – uiteindelijk leiden tot een controlesamenleving, surveillancestaat of social creditsysteem. Daarom dienen proportionaliteit, 'ethics by design' en 'privacy by design' leidende principes te zijn bij het nadenken over toepassing van technologie door de overheid.

Verkeersveiligheid en verkeershandhaving in de toekomst

Zelfrijdende auto's, e-bikes en intelligente wegkantsystemen hebben effect op de verkeersveiligheid, maar leiden ook tot nieuwe verkeershandhavings- en reguleringsvraagstukken. Smartphones, apps en straks augmented reality kunnen zorgen voor afleiding in het verkeer, maar ze kunnen ook helpen bij navigatie. De verkeersveiligheid kan daarentegen ook worden vergroot door bijvoorbeeld de inzet van kunstmatige intelligentie voor ongevallenpredictie. Of doordat televergaderen simpelweg leidt tot minder mobiliteit en daarmee een lagere kans op ongevallen. Maar er ontstaan ook nieuwe juridische vragen, omtrent de regulering, aansprakelijkheid en handhaving van bijvoorbeeld zelfrijdende auto's, elektronische eenwielers, jetsuits, passagiersdrones of vliegende auto's. Ook de toegang tot betrouwbare forensische data van boordcomputers of intelligente wegkantsystemen bij verkeersongevallen is van belang voor de politie. Tot slot kan beeldherkenning helpen bij verkeershandhaving. Wel is daarbij ook weer proportionaliteit een belangrijk aandachtspunt.

> Diverse technologieën maken het **wederzijdse contact** tussen **burger** en **politie gemakkelijker**

Data en intelligence voor politiewerk

Het slimmer omgaan met data, meer informatie halen uit data en zorgen dat intelligence op het juiste moment op de juiste plek belandt, zodat de juiste keuzes worden gemaakt, is van essentieel belang voor het politiewerk. Technologische ontwikkelingen leiden ertoe dat er steeds meer informatiebronnen en brondata beschikbaar komen: zowel socialmediadata, IoT-data als sensingdata. Technieken als privacy enhancing technologies maken het ook beter mogelijk om data uit te wisselen tussen verschillende organisaties. Met kunstmatige intelligentie, tekstanalyse, knowledge graphs en simulatie- en datavisualisatietechnieken ontstaan nieuwe manieren om data te analyseren. Data-analyse kan bovendien steeds sneller plaatsvinden, door de toename van rekenkracht, data-analytics en quantum computing. Data kunnen gemakkelijker en sneller worden overgedragen, door middel van 5G, smartphones en apps. Daarnaast zijn er nieuwe manieren om data te presenteren of te visualiseren, bijvoorbeeld via VR, augmented reality of wearables. Beslisalgoritmes of profilingalgoritmes kunnen helpen bij de juiste besluitvorming op basis van de data. Met name big data, sensoren en AI bieden (potentieel) grote kansen om overheidsinterventies gerichter, efficiënter en rechtvaardiger te laten verlopen. Hoe meer data er bekend is, hoe beter alle omstandigheden van het geval in de besluitvorming kunnen worden betrokken. Wel is belangrijk dat de technologie proportioneel wordt ingezet en dat er een goede balans is tussen privacy en ethische normen. Tegelijkertijd zijn er ook risico's bij datagebruik. Door verkeerde datasets of verkeerd toegepaste algoritmes kunnen fouten in besluitvorming ontstaan. Momenteel wordt er veel beleidsmatige aandacht besteed aan het voorkomen van dergelijke fouten. Daarnaast is informatie-overload een risico. Tot slot is er ook het risico van gemanipuleerde of onware data of informatie; bijvoorbeeld door toepassing van synthetische media of bots.

Technologie voor opsporing

Met name voor de opsporing bieden technologische ontwikkelingen zeer veel nieuwe mogelijkheden. In de eerste plaats leidt technologie tot nieuwe soorten (digitale) sporen, door nieuwe toepassingen die op de markt komen (wearables, persoonlijke assistenten, domotica, VR/AR-brillen, drones, autonome systemen, zelfrijdende auto's, sensoren). Daarnaast: hoe meer mensen gebruik maken van nieuwe toepassingen, hoe meer data (en potentiële) sporen er ontstaan. Denk aan de toename van het aantal smartphones, camera's, bodycams en dashcams, uitbreiding social media en dark web, cloud-data, locatiegegevens, WiFi-tracking, cryptocurrencies. Technologische ontwikkelingen maken het ook mogelijk om meer informatie uit sporen te halen (DNA-analyse, scherpere camerabeelden, beeldanalyse, gezichtsherkenning, stemherkenning, voice-to-face, quantum). Daarnaast maakt technologie snellere analyse van sporen mogelijk (sensor en nanotechnologie: labs-on-chips, kunstmatige intelligentie, mobiele technologie, apps, data-analytics, beeldherkenning, spraakherkenning), alsmede betere selectie van sporen (bijvoorbeeld via AI). Ook zijn er nieuwe manieren om sporen te vergaren (beelden uit de lucht via satellieten, drones, wide-area motion imagery, onderwaterdrones voor opsporing onder water, inzet van drones en robots om contaminatie van de plaats delict te voorkomen), nieuwe manieren om met bewijs om te gaan (via VR of blockchain), maar ook nieuwe manieren om cold cases op te lossen (AI, deepfakes). Ook voor speciale operaties kan techniek worden ingezet; denk aan 3D-printing, sensoren en robotica voor observatie of intelligente wegkantsystemen voor achtervolgingen. Anderzijds maakt technologie het in toenemende mate mogelijk voor burgers zelf om zaken op te sporen (social media, domotica, (mini)camera's, locatiesensoren, gezichtsherkenning, DNA-analyse). Daarnaast kan er valse of onware informatie zijn, door manipulatie van audiovisueel materiaal via deepfakes, spoofing van DNA of manipulatie van herinneringen via VR. Of

kunnen ontwikkelingen als kwantumcommunicatie het moeilijker maken om informatie te onderscheppen, of kan domotica ervoor zorgen dat heimelijke operaties worden bemoeilijkt.

Agent van de toekomst

Technologie kan op diverse manieren bijdragen aan de agent van de toekomst (of de veiligheidsprofessional in brede zin). In de eerste plaats kan technologie bijdragen aan een goede digitale uitrusting (smartphone, 5G, apps, wearables) en informatiepositie (door VR, AR, simulatie, beeldtafels, spraakherkenning, persoonlijke assistent en beslisalgoritmes). Daarnaast draagt technologie bij aan de fysieke uitrusting (bodycams, smart kleding, beschermende kleding, gehoorbescherming, exoskeletten, niet-dodelijke wapens) alsook mobiliteit (nieuwe vervoermiddelen, navigatie, dashcams). Ook kan technologie bijdragen aan de ondersteuning van veiligheidsprofessionals (drones, onderwaterdrones, robots, sensoren). Technologie kan worden ingezet voor opleiding en training (VR, AR, telepresence, apps, simulatie, adaptief leren met AI, serious gaming), maar ook voor duurzame inzetbaarheid (wearables, VR). Daarnaast kan technologie worden ingezet voor werving en selectie (gaming, AI, telepresence).

Politie op het web (dienstverlening, digitale wijkagent)

Diverse technologieën maken het wederzijdse contact tussen burger en politie gemakkelijker. Voor de toegankelijkheid van de politie kunnen social media, webcare, vertaalalgoritmes, ontvangstrobots of synthetische collega's worden ingezet. VR, XR of telepresence maakt service op afstand mogelijk. Daarnaast zijn er nieuwe domeinen waar de politie op aanwezig kan zijn, zoals in games of de metaverse. Hier kunnen bijvoorbeeld kwetsbare groepen worden bereikt. Ook zijn er nieuwe kanalen voor de bereikbaarheid van de politie, zoals persoonlijke assistenten als Siri of Google Home of wearables. Gerichtere service kan worden geboden via chatbots of beslisalgoritmes en snellere afdoening is mogelijk met behulp van spraakherkenning, taalanalyse, self sovereign identity en knowledge graphs.

Politie en bedrijfsvoering

Technologie kan bijdragen aan duurzaamheid door elektrisch rijden, vergaderen op afstand, autodeelapps en zonnepanelen. Onderhoud en onderhoudsdetectie kan door middel van mobiele data, sensoren, AI, predictieve analyses, 3D-printing. Met water- en vuilafstotende coatings en schoonmaakrobots kan worden bespaard op schoonmaakkosten.

> Het is **belangrijk** dat er een goede **balans** is tussen **privacy** en **ethische normen**

Kortom

Duidelijk is dat technologische ontwikkelingen het politiewerk in alle opzichten raken. Om hier goed op in te spelen is het van belang om aandacht te hebben voor de 'organisational readiness' van de politie.
Nieuwe vormen van criminaliteit of nieuwe veiligheidsdreigingen, maar ook nieuwe mogelijkheden voor opsporing en intelligence betekenen bijvoorbeeld dat specifieke capaciteit en expertise nodig is om hiermee om te kunnen gaan. Dat geldt bijvoorbeeld voor voldoende capaciteit en expertise op het gebied van AI, data-analyse, privacy enhancing technologies, crypto- en kwantumtechnologie, maar ook juridische expertise op het gebied van data-ethiek-compliance. De politieorganisatie verandert voortdurend qua samenstelling, door uitstroom en nieuwe instroom. Maar ook opleiding en training zorgen voor beter toegeruste expertise en capaciteit binnen de politieorganisatie. Daarnaast is het ook belangrijk dat de juiste kennis wordt ontwikkeld en dat de politie waar nodig is aangesloten bij state-of-the-art kennis en technologie. Verder moet op technologiegebied goede samenwerking plaatsvinden met nationale en internationale experts. Waar nodig moeten aanspreekpunten en leads duidelijk zijn. Het experimenteren en opschalen van kansrijke technologische innovaties moet worden gestimuleerd, uiteraard met inachtneming van principes van proportionaliteit en ethiek. In de Science & Technology agenda van de politie worden al deze zaken geadresseerd. •

Veiligheid regisseren in de sensorsamenleving

HET AANTAL TOEPASSINGEN GROEIT STERK

Aan beveiligingscamera's, agenten met bodycams en smartphonefilmende omstanders zijn we inmiddels gewend. Maar er zijn meer manieren om onveilige situaties te signaleren. Objecten, slimme apparaten, voertuigen: alles kan voorzien worden van digitale sensoren die al lang meer kunnen dan alleen zien en horen. Deze extra zintuigen verrijken het 112-meldproces en de opvolging ervan in ons land, zeker als de data die zij genereren slim gekoppeld en geanalyseerd worden. Wat kan sensing voor de meldkamer van de toekomst betekenen? Welke rol heeft de burger bij dit 'nieuwe melden'? Welke verandering staat onze samenleving te wachten om de mogelijkheden die de technologie biedt daadwerkelijk te omarmen en hoe verhoudt zich dit met onze behoefte aan privacy?

Over de auteur
Frank Wieland is Director Consulting Expert bij ICT-dienstverlener CGI. Daarnaast is hij Expert voor de Politie, als onderdeel van de portefeuille Digitalisering (deelprogramma Sensing).

Tekst: Frank Wieland • Foto: Unsplash

Het is een cliché, maar de technologische ontwikkelingen en digitalisering van de samenleving gaan razendsnel. Het geschetste beeld van de meldkamer van de toekomst (zie hiernaast) is dichterbij dan je zou denken. Zo zijn er inmiddels in Nederland al meer dan anderhalf miljoen beveiligingscamera's van bedrijven en particulieren actief, naast vele duizenden toezichtcamera's van de gemeenten en van de politie. En dat is nog zonder alle smartphones en andere sensoren. Bedrijven en particulieren filmen hun omgeving met slimme deurbellen. Op de autoweg filmen zij het verkeer met dashcams. De gemeente gebruikt slimme camera's die nummerborden kunnen 'lezen'. De agenten dragen bodycams; burgers filmen en fotograferen elkaar, 24 uur per dag. En ja, ook de slimme lantaarnpaal uit het toekomstbeeld bestaat al. De paal meet in de openbare ruimte onder meer het geluidniveau om in de gaten te houden of er ergens ruzie ontstaat.

Meer zintuigen, meer mobiliteit

De technologische ontwikkelingen op het gebied van sensing worden voor een belangrijk deel veroorzaakt door steeds kleiner wordende chips met grote rekenkracht die tevens energiezuinig zijn. Hiermee kunnen we allerlei soorten goederen en objecten steeds slimmer maken. Daar waar traditionele beeldcamera's en microfoons voorheen alleen konden 'kijken'

en ‘horen’, is de technologie inmiddels zo ver dat digitale sensoren ook zelfstandig kunnen ‘ruiken’, ‘proeven’ en ‘voelen’ en in combinatie meerdere dingen tegelijk kunnen doen.

Digitale getuigen

Met digitale sensoren die steeds meer kunnen en bovendien mobieler worden, groeit het aantal toepassingen. Zo kunnen de sensoren voor de gemeenten en hulpdiensten als de politie uitstekend fungeren als getuigen van situaties in de samenleving waarin leefbaarheid of veiligheid onder druk staat. Door verzamelde sensordata automatisch te verrijken met informatie uit andere databronnen kan bijvoorbeeld een verdacht gedrag of patroon in de samenleving al in een vroeg stadium worden gesignaleerd. Zo zette de politie de afgelopen jaren intelligente camera’s in om het aantal vrachtwagen- en ladingdiefstallen in Nederland terug te brengen. De politie gebruikte op afstand bestuurbare ‘dome’-camera’s, infraroodcamera’s en ANPR-camera’s (nummerbordherkenning) om automatisch ladingdiefstal op snelwegen en parkeerplaatsen te detecteren.

De gemeenten en politie maken voornamelijk gebruik van sensoren die geplaatst zijn in de publieke ruimte. Private partijen (burgers en bedrijven) zetten eveneens sensortoepassingen in, met name bedoeld om eigendom en een werk- en/of leefomgeving te monitoren. Ook de individuele burger kan daarbij als een (informatie)sensor worden beschouwd. Zo toonde het programma Burger Alert Real Time! (BART!) aan dat buurtpreventieteams bereid zijn digitale informatie (sociale media: tekst, foto, video) real-time te delen met de gemeente en politie, zodat zij bij het signaleren van leefbaarheid- of veiligheidsproblemen in samenwerking kunnen handelen. Zolang dit de veiligheid ten goede komt, vindt de burger het geen probleem dat de eigen omgeving met sensoren wordt gemonitord (bron: Rathenau Instituut).

> “Digitale sensoren kunnen ook zelfstandig ‘**ruiken**’, ‘**proeven**’ en ‘**voelen**’

Nog geen structurele inzet

Als je dit leest, lijken alle seinen op groen te staan om bijvoorbeeld onze opsporingsdiensten datagedreven te laten werken. Deze diensten gaan er zelf al van uit dat in de toekomst ongeveer negentig procent van de (geautomatiseerde) informatiestromen afkomstig zal zijn van private en publieke sensoren. Met deze sensoren kunnen continu data uit de samenleving worden verzameld, geanalyseerd en toegepast. Technologisch gezien staan we al met één been in de sensorsamenleving. Toch blijft vooralsnog de structurele inzet van sensortechnologie, big data en artificial intelligence voorbehouden aan incidentele operaties, zoals het terugbrengen van het

De meldkamer van de toekomst

Het is het jaar 2030. We bevinden ons in de meldkamer van de hulpdiensten. Hier geen rinkelende telefoons en centralisten die bij elk binnenkomend 112-belletje moeten beslissen of er een hulpdienst ingeschakeld moet worden en zo ja, welke. De meldkamer wordt bemenst met veiligheidsregisseurs die alle benodigde informatie aangereikt krijgen van het digitale meldsysteem dat gevoed wordt door allerlei sensors. Zo registreerde zojuist een slimme lantaarnpaal een schot. De veiligheidsregisseur die deze melding ziet, stuurt alvast een ambulance en een politieauto naar de bewuste locatie, terwijl we in de meldkamer livebeelden ontvangen van diverse camera’s in de buurt. Aan de hand van artificial intelligence worden de beelden geregistreerd en geanalyseerd. Op een van de camerabeelden blijkt een gestrekte arm te zien, met iets in de hand dat op een wapen lijkt. Met gezichtsherkenning in de camera’s wordt gekeken naar de mogelijke dader en de richting gevolgd waarin deze is gelopen. Ook het slachtoffer is in beeld. Diens smartwatch registreert een val, een oplopende hartslag en verlaagde saturatie in bloed. Een van de omstanders neemt contact op met de meldkamer en start een videocall. De veiligheidsregisseur kan op basis van alle input adequaat schakelen met politie en het ambulancepersoneel die onderweg zijn. We kijken vervolgens real-time mee naar het werk dat de hulpdiensten verrichten om de veiligheid te waarborgen. Door de inzet van augmented reality voelt het alsof we ons midden in de werkelijke situatie bevinden…

De komende jaren worden dit de bepalende kenmerken van de sensorsamenleving:

1. De toenemende mate en inzet van verschillende nieuwe vormen van interactieve, genetwerkte sensoren overal in de samenleving (IoT);
2. De toename in het volume van door alle sensoren gegenereerde digitale datastromen (Big Data) bestemd voor opsporingsdiensten;
3. De ontwikkeling en toepassing van voorspellende analyses om op real-time basis enorme hoeveelheden datagegevens tot bruikbare informatie te verwerken (AI);
4. Het verwerken en inzichtelijk en begrijpelijk maken van geanalyseerde datagegevens om daar als opsporingsdienst gericht opvolging aan te kunnen geven (Sense Making).

> Het moet **helder** zijn dat de **burger** kan **bijdragen** aan onze **veiligheid**

aantal vrachtwagen- en ladingdiefstallen. Dat komt doordat het digitaliseren van onze samenleving gepaard gaat met soms lastige sociale, juridische en ethische vraagstukken. Technologie is hier niet de doorslaggevende factor. Het samenspel tussen onze overheid en de burger is dat wél.

Begrijpelijke data-ecosystemen

De inzet van nieuwe technologieën en het (nog meer) verzamelen van data in de openbare ruimte botsen met het belang van privacy, zeker als het voor de burger onduidelijk is wat het doel is van al die sensoren. Het moet helder zijn dat de burger kan bijdragen aan onze veiligheid. Dat elke melding belangrijk kan zijn. Dan moet er wel een concrete opvolging zijn. Zoals bij Burgernet, waarbij iedereen die mee heeft gedaan aan een actie na afloop een appje krijgt met het resultaat ervan. Hierdoor krijgt de burger het gevoel dat hij heeft bijgedragen aan de veiligheid.

Deze lijn zou ook doorgetrokken moeten worden in de meldkamer van de toekomst. We gaan van de klassieke centralist die in de meldkamer de telefoon aanneemt, luistert en bepaalt of de politie, de brandweer of een ambulance ingeschakeld moet worden, naar de veiligheidsregisseur die een richting aangereikt krijgt van een datagedreven systeem gevoed door sensorinformatie. We gaan van een burger die zich gecontroleerd voelt naar een burger die zelf bijdraagt aan de controle. Dat is een majeure transformatie. Maar wel een waarbij de overheid kan helpen onze samenleving zo leefbaar en veilig mogelijk te houden.

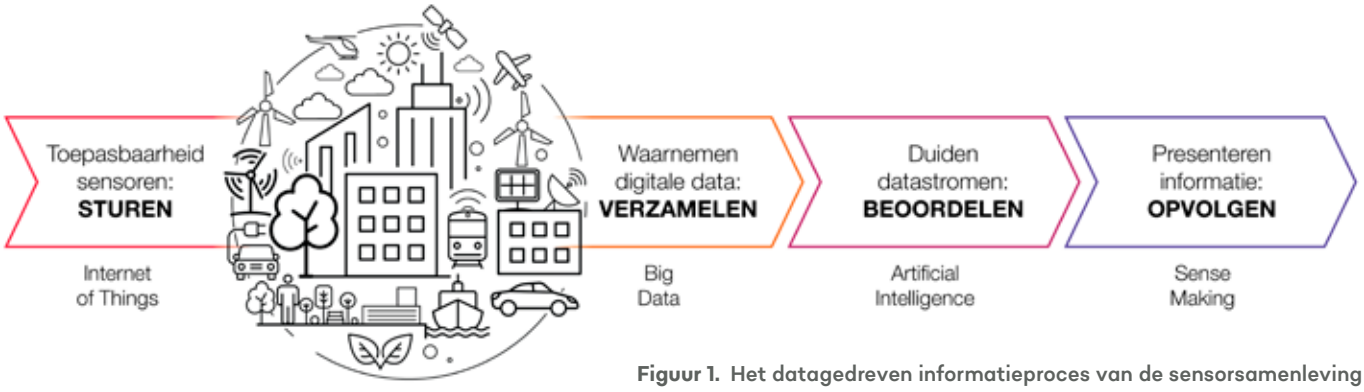
Wat staat de politie te wachten?

Bij het inzetten van sensortoepassingen gaat het voor de politie vaak om het ondersteunen van de operationele processen, op locaties in de samenleving waar de (continue) behoefte bestaat om informatie in te winnen. Deze toepassingen verzamelen daarbij veel data, die vaak betrekking hebben op personen. Maar wat zijn de gevolgen van deze sensortoepassingen voor de rechten en vrijheden van burgers, waaronder de bescherming van persoonsgegevens?

AVG zegt nee

Vooropgesteld: bij het inzetten van sensortoepassingen mag de overheid geen inbreuk maken op de directe levenssfeer of vrijheden van de burger. De algemene verordening gegevensbescherming (AVG) is daar glashelder in en verbiedt het onnodig of ongeoorloofd verzamelen of gebruiken van persoonsgegevens (Art. 5 AVG). Bovendien moeten burgers vooraf geïnformeerd worden over hoe en waarvoor de verkregen informatiegegevens worden gebruikt (Art. 13 AVG). Daarbij moeten zij ook inzage kunnen krijgen in de dataverzameling, indien zij daartoe de overheid verzoeken (Art. 15 AVG).

Maar nog belangrijker: de AVG kent ook als uitgangspunt dat niemand onderworpen mag worden aan een uitsluitend op geautomatiseerde verwerking gebaseerde beslissing waaraan voor de burger belangrijke (rechts)gevolgen zijn verbonden (Art. 22 AVG).



Figuur 1. Het datagedreven informatieproces van de sensorsamenleving

Technologisch gezien gaat het bij het inzetten van sensortoepassingen in de samenleving daarom vooral over de aanpak. Hierbij kan de overheid het verzamelen van data (sensoren) in combinatie met gebruik van artificial intelligence/machine learning op een verantwoorde wijze toepassen zónder de AVG daarbij te schaden ('automatisch stigmatiseren van bepaalde groepen of burgers in de samenleving op basis van (alleen) technologische sensorprofielen kan niet/mag niet – de mens neemt hier op basis van informatie een besluit – v.w.b. de politie: wel of geen opvolging geven').

Sociaal versus individueel belang

Ethisch gezien dient onze samenleving de vraag te beantwoorden of leefbaarheid en veiligheid voor bewoners in een buurt of wijk zwaarder wegen dan bijvoorbeeld de (individuele) privacy van een burger. Ofwel: wat is het de burger waard om te leven in een leefbare en veilige omgeving? En in hoeverre is die burger bereid om informatie uit de eigen omgeving te delen met bijvoorbeeld de overheid? In buurten en wijken in Nederland waar buurtpreventieteams actief zijn, bepalen de burgers dit zelf. Ze kiezen er ook zelf voor of zij in digitaal opzicht met de overheid verbonden willen worden, bijvoorbeeld in het kader van het al eerdergenoemde Burger Alert Real Time!.

Veiligheid regisseren

2023 wordt voor de politie het overgangsjaar naar het gebruik van de generieke sensingvoorziening. Met behulp van het zogenaamde Sensing Platform is de politie dan in staat om op real-time basis datastromen te verzamelen uit verschillende soorten sensortoepassingen. Hierbij worden de verzamelde data op eenduidige wijze verwerkt ter ondersteuning van alle operationele politieprocessen ('Sense Making'). Als eerste sensortoepassing komt in 2023 (het huidige gebruik van) automatische nummerplaatherkenning (ANPR) voor de politie beschikbaar, inclusief de integratie van de functionaliteiten Falconi en i-Trechter. Daarna volgen steeds meer sensoren en sensortoepassingen de weg naar dit platform. Als het gaat om het regisseren van veiligheid, dan is het Sensing Platform daarmee voor de politie voorbereid om als digitale verbinding naar de samenleving te fungeren. Het ondersteunt dan de meldkamers real-time in informatie en in de samenwerking tussen de burger en de politie.

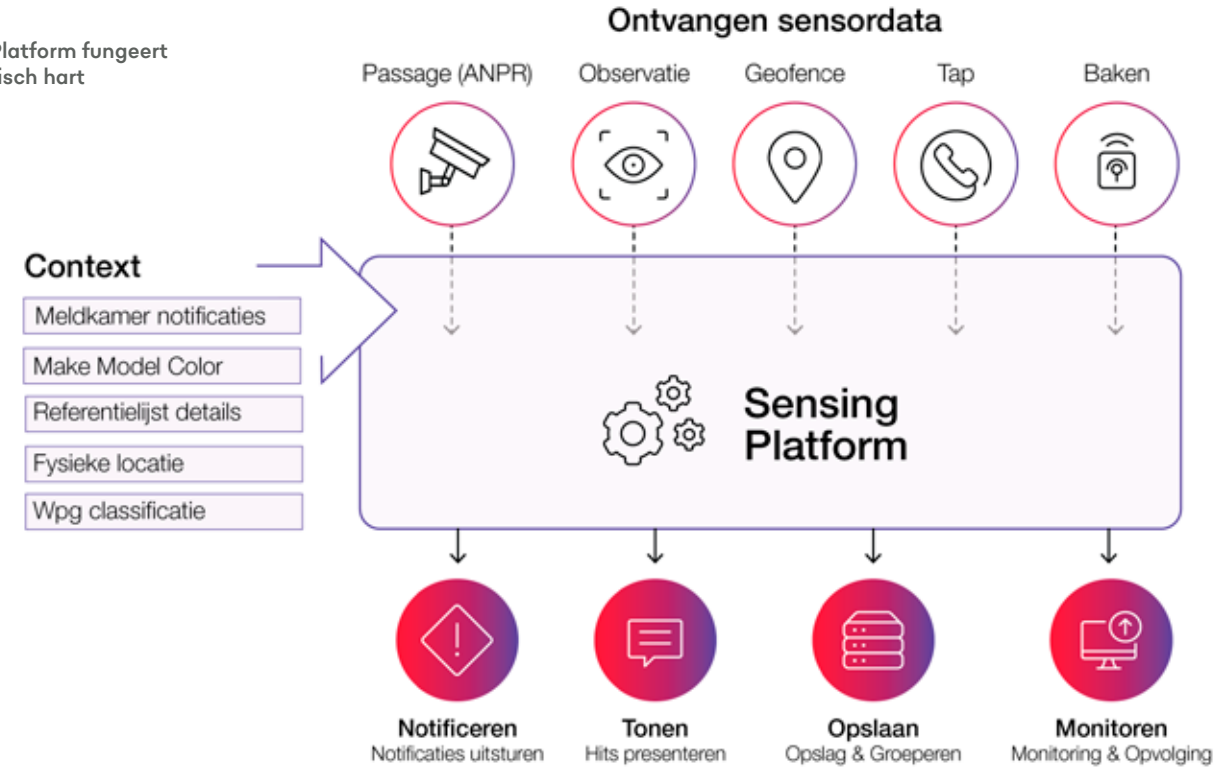
> Het **digitaliseren** van onze samenleving gaat gepaard met **lastige** sociale, juridische en ethische **vraagstukken**

Het Sensing Platform

Het Sensing Platform is voor de politie een verzameling van technologische services met als doel het faciliteren van bruikbare informatie, afkomstig uit de verwerking van sensorwaarnemingen in de samenleving. Het Sensing Platform fungeert hiermee voor de hele politieorganisatie als technologisch hart. Het Platform is automatisch in staat om de verzamelde sensorwaarnemingen (data) te verrijken met informatie uit verschillende politiesystemen, vervolgens op generieke wijze te duiden in de (politie)context (bijvoorbeeld automatische toetsing op het voorkomen daarvan in een referentielijst of profiel), te classificeren ('handhaving, opsporing, anders'), te prioriteren ('spoed, nu, later') en te notificeren naar 'het juiste loket' voor de opvolging (hit, no hit: Eenheid, Dienst, Team, Diender). Bij het ontwerpen en realiseren van dit platform is het 'privacy-by-design'-principe toegepast. Het resultaat is een toekomstbestendige sensingomgeving waarin allerlei soorten sensoren en sensortoepassingen kunnen worden ondergebracht. Het platform is voorzien van gestandaardiseerde organisatiebouwstenen op basis waarvan meerdere sensingtoepassingen voor de politie kunnen worden ontwikkeld (sensortechnologieën, infrastructuren en IV-standaarden). In het platform worden alle functies geïntegreerd die nodig zijn om de (sensing)producten en diensten te leveren aan de eindgebruiker. Het werken met sensoren in de samenleving kan daarmee op een eenduidige (werk)wijze worden ondersteund, ten bate van alle operationele politieprocessen binnen de politieorganisatie.

De rol van informatiemanagement

Gedurende de tweede helft van 2022 treft het Politiedienstencentrum (PDC, Dienst Informatiemanagement) voorbereidingen waarmee vanaf 2023 het Sensing Platform voor alle politie-eenheden kan worden geïmplementeerd/geoperationaliseerd. Is het Sensing Platform eenmaal beschikbaar? Dan zullen er steeds meer (andere) sensoren, sensorvoorzieningen en sensingfunctionaliteiten op dit platform worden aangesloten met als doel de politie-operatiën maximaal in informatie te ondersteunen met een rechtvaardig gebruik van sensoren in de samenleving. Het PDC (Dienst Informatie Management) begeleidt daarbij de digitale transformatie voor de politie-eenheden, op weg naar het operationele gebruik van het Sensing Platform.



Figuur 2.
Het Sensing Platform fungeert als technologisch hart

Dr. Gwen van Eijk
Criminoloog en onderzoeker en beleidsmedewerker Technologie en Mensenrechten bij Amnesty International Nederland

De geloofwaardigheid van voorspellende technologieën

Als het gaat over voorspellende technologieën zoals *predictive policing* en geautomatiseerde risicoprofilering, is een verwijzing naar het verhaal *Minority Report* van Philip K. Dick uit 1956, verfilmd in 2002, nooit ver weg. En dat terwijl onze technologieën die criminaliteit proberen te voorspellen weinig te maken hebben met drie *precogs* – helderzienden – wier hersenen zijn aangesloten op een computer. Toch zijn er wel parallellen, niet vanwege de technologie maar vanwege de manier waarop overheden ermee omgaan. In het oorspronkelijke verhaal zien de drie precogs meestal *niet* dezelfde toekomst en is er enige discussie over het opsluiten van onschuldige burgers. In de verfilming zit het net even anders: de drie zien meestal *wel* dezelfde toekomst, maar soms wijkt één van hen af. Dit wordt voor burgers geheimgehouden, uit angst dat deze informatie de geloofwaardigheid van het systeem zou ondermijnen.

Op welke verhaalvariant lijkt onze realiteit het meest? Het is geen geheim dat voorspellende technologieën niet honderd procent accuraat zijn, maar er is weinig discussie over de implicaties daarvan. En ook onze overheden zijn weinig open over de inzet en werking van risicoprofilering. Waar de protagonist van *Minority Report* zijn leven op het spel moet zetten om de waarheid boven tafel te krijgen, zijn het in onze realiteit politici, journalisten en activisten die met Tweede Kamermoties, Wob-verzoeken en inzageprocedures inzicht proberen te verkrijgen, lang niet altijd met succes. Zowel bij de politie als bij andere overheidsinstanties – zie het Toeslagenschandaal en de discussie over SyRI – zien we een gebrek aan transparantie.

> Voor de burger valt of staat de **geloofwaardigheid** van overheidsoptreden met **rechtszekerheid** en **verantwoording**

In een rechtsstaat hebben burgers het recht te weten welke beslissingen overheden over ze nemen en hoe deze tot stand komen, en om ze te weerleggen als ze niet juist zijn. Dit is niet makkelijk wanneer een beslissing is genomen mede op basis van een (onjuiste) voorspelling. Ten eerste weten burgers vaak niet dat er een risicoprofiel is gebruikt. Ten tweede kan het moeilijk of zelfs onmogelijk zijn om te begrijpen hoe een voorspelling over iemand tot stand is gekomen. Dit laatste speelt vooral wanneer zelflerende algoritmen worden losgelaten op een steeds grotere hoeveelheid persoonlijke gegevens – van beelden en sociale mediaberichten tot reisgegevens en financiële transacties. De link tussen gegevens en voorspelling is steeds moeilijker te traceren.

Nu zullen overheden tegenwerpen: "Er komt altijd een mens aan te pas om de voorspelling te duiden en waar nodig te corrigeren." De vraag is of dit voldoende garantie biedt. Zonder transparantie weten we namelijk óók niet hoe overheden omgaan met fouten. Een veelgehoord argument tegen transparantie is dat het 'gaming the system' in de hand werkt. Maar misschien is er ook wel, net als in *Minority Report*, een angst dat openheid over foute voorspellingen de geloofwaardigheid van risicoprofilering ondermijnt. Dan is het goed te blijven beseffen dat voor de burger de geloofwaardigheid van overheidsoptreden valt of staat met rechtszekerheid en verantwoording. Transparantie, ook over fouten, is daarvoor essentieel. •

→ Reageren? G.vaneijk@amnesty.nl

Wat is de rol van de politie bij metaverse?

HET RATHENAU INSTITUUT ONDERZOEKT DE MAATSCHAPPELIJKE RISICO'S

Leven we over vijftien jaar in een virtuele wereld? Dringt de digitale wereld door tot in onze huiskamers? Kunnen we nog nep van echt onderscheiden? Wie is verantwoordelijk voor als er iets misgaat en wie moet er handhaven? Vragen die steeds vaker klinken sinds het najaar van 2021. Facebook veranderde destijds haar naam in Meta, maar ook Microsoft, Apple en Epic kondigden grootse investeringen aan.

Kortom, de metaverse staat volop in de belangstelling, maar er is nog veel onduidelijk. Om een beeld te geven van de investeringen die momenteel gaande zijn: consultancybedrijf Mckinsey berekende dit jaar dat de totale investeringen in 2021 rond de dertien miljard dollar bedroegen, en dat deze investeringen over 2022 halverwege het jaar al meer dan verdubbeld waren.[1] Het moge duidelijk zijn: velen proberen een graantje mee te pikken van deze trend.

Een virtuele omgeving waarin het online en echte leven overlappen

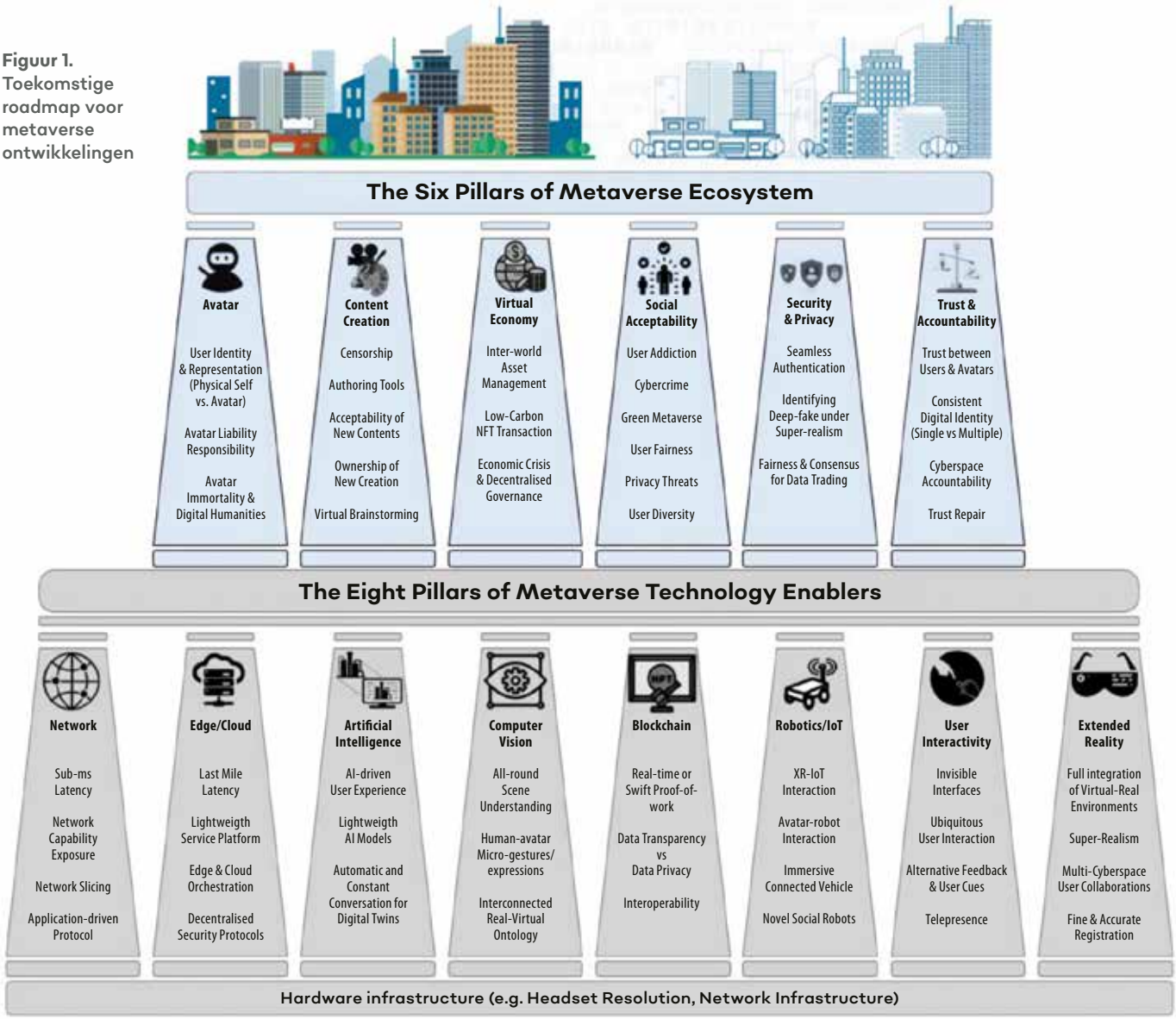
In deze benadering vormt de metaverse een toekomstige digitale wereld waarin je nog meer verbondenheid voelt met het echte leven en je echte lichaam, door toepassing van immersieve technologieën.[2] Immersieve technologieën zijn technologieën waarbij je het gevoel krijgt dat je fysiek bent ondergedompeld in een digitale wereld. Voorbeelden zijn virtual reality, augmented reality en spraaktechnologieën. Je zou bijvoorbeeld evenementen kunnen bezoeken, gaan winkelen en virtueel op je kantoor kunnen werken in de metaverse. Deze activiteiten zullen immersiever en realistischer zijn dan onze ervaringen op het huidige internet.

Een volgende stap in het creëren van een virtuele economie

In deze benadering ligt de nadruk op het ontstaan van een virtuele economie. Het is de virtuele wereld van de Blockchain[3], Cryptocurrencies[4] en NFT's[5] waar ontwerpers virtuele objecten kunnen maken, eigendom hierover kunnen claimen en kunnen handelen. Deze kansen voor handel in virtuele objecten maakt het voor veel bedrijven ook aantrekkelijk om een rol te spelen in de metaverse. Omdat veel elementen van deze virtuele economie al bestaan, vinden sommigen dat de metaverse daardoor ook al bestaat. De bekendste voorbeelden die hierbij worden aangehaald zijn Decentraland en the Sandbox. Dit zijn online werelden waar je als avatar kan rondlopen en land en kunstwerken kan kopen en verkopen.

Over de auteurs
Stefan Roolvink MSc is onderzoeker bij het Rathenau Instituut in Den Haag.
Sanderijn Kuijvenhoven is stagiair bij het Rathenau Instituut in Den Haag.
Dr. Mariette van Huijstee is onderzoekscoördinator bij het Rathenau Instituut in Den Haag.

Tekst: Stefan Roolvink, Sanderijn Kuijvenhoven & Mariette van Huijstee • Foto: VR Training Academy, Enschede



Figuur 1.
Toekomstige roadmap voor metaverse ontwikkelingen

De metaverse als sociaal-digitale infrastructuur

Verschillende onderzoekers en kennisinstituten beschrijven de metaverse als samenraapsel van sociale en technologische puzzelstukjes. Een voorbeeld is het model van onderzoekers Lik-Hang Lee et al. van de University of Helsinki. Zij presenteren maar liefst veertien aspecten die samen de metaverse zullen vormen of nodig zullen zijn om de metaverse te creëren (zie figuur 1). Het model illustreert de veelzijdigheid van de (discussie over) de metaverse, inclusief mogelijke verdienmodellen.

Maatschappelijke risico's

De verschillende benaderingen van de metaverse roepen een hoop vragen op over de maatschappelijke impact. Waar is deze te verwachten en hoe wordt hierover gesproken door investeerders, journalisten en tech-experts? Op de website van het Rathenau Instituut zijn rapporten te downloaden waarin risico's van verdere digitalisering en het gebruik van virtual en augmented reality in beeld worden gebracht.[6] Daarnaast zijn er steeds meer investeerders, journalisten en tech-experts die hierover nadenken. Dit zijn ook mogelijk relevante vragen voor de politie.

Biometrische surveillance: risico's voor ons recht op privacy

Voor het creëren van realistische virtuele werelden zijn persoonlijke data van gebruikers nodig. Deze data worden verzameld via bijvoorbeeld camera's en slimme speakers. Deze data kunnen vervolgens gebruikt worden voor verregaande individuele profilering. Omdat AR

1 Mckinsey & Company (2022). Value Creation in the Metaverse, p. 7.
2 Robertson, A., & Peter, J. (2022) *What is the metaverser? And why do I have to car?*
3 Blockchaintechnologie is een technologie waarmee data – informatie – opgeslagen worden in een keten van blokken waarbij deze blokken niet gewijzigd kunnen worden. De blokken bevatten ieder informatie en ook een versleutelde versie van de informatie op andere blokken.
4 Cryptomunten zijn digitale munteenheden gebaseerd op de blockchain. Op de blockchain worden ook de digitale transacties geregistreerd.
5 NFT's zijn op de blockchain geregistreerde eigendomscertificaten (tokens) met een unieke ID gekoppeld aan een onderliggend goed. Deze NFT's kunnen van alles zijn. Denk aan een stuk virtueel land, je eigen avatar en accessoires voor je avatar, maar ook kunst of muziek. De waarde van een NFT is afgeleid van het feit dat deze niet-inwisselbaar zou zijn.

> Een brede **maatschappelijke discussie** is wenselijk

Rathenau Instituut

Het Rathenau Instituut doet vanuit haar rol als *technology assessment* instituut in 2022 onderzoek naar de maatschappelijke risico's in de metaverse. Daarnaast willen het instituut het gesprek in de samenleving hierover stimuleren. We hebben namelijk nu de mogelijkheid om de ontwikkeling in goede banen te leiden en daar maatschappelijk debat over te voeren. Het gesprek over deze maatschappelijke risico's komt nauwelijks op gang. Het instituut wil daarom makers, ontwikkelaars, maatschappelijke organisaties en overheden stimuleren om het gesprek aan te gaan: welke aspecten van de metaverse vinden we vanuit maatschappelijk oogpunt wenselijk en welke vinden we minder wenselijk? Wat moet er nu gebeuren om de ontwikkeling in goede banen te leiden, en wie is daarbij aan zet? En wie bewaakt de veiligheid straks in de metaverse? Dit zijn ook belangrijke vragen voor de politie.

veelal wordt gebruikt in een sociale context, zoals in de publieke ruimte, geeft de benodigde dataverzameling direct aanleiding tot een aantal privacyvraagstukken. Denk hierbij aan het gebruik van gezichts- en gedragsherkennende camera's of slimme AR-brillen zoals de Google Glass. Deze werd in 2015 mede wegens privacybezwaren vanuit maatschappelijke organisaties en potentiële klanten alweer van de markt gehaald.

Digitale modificatie: vervaging van nep en echt

De toegang tot informatie kan worden bedreigd door de toepassing van immersieve technologieën. Een veelgebruikte toepassing van bijvoorbeeld VR en AR is het zo levensecht mogelijk nabootsen, aanpassen of wegfilteren van landschappen, gebouwen en zelfs mensen. Klaslokalen en stadsparken kunnen worden nagebootst, verrijkt of verarmd met virtuele objecten. Dit kan ons gedeelde beeld van de werkelijkheid beïnvloeden. In ons rapport 'Digitale dreigingen voor de democratie'[7] beschrijven we hoe deepfakes en desinformatie kunnen leiden tot gefragmenteerde wereldbeelden. De vraag is kortom hoe we in de toekomst nog een gezamenlijk beeld van de werkelijkheid hebben en of we het verschil tussen 'echt' en 'nep' nog kunnen onderscheiden.

Risico's voor digitale en fysieke integriteit

Waar de meeste mensen nu online interageren via 'klassieke' tools zoals het toetsenbord, muis of consolecontrolers, zal in de metaverse de interactie met je omgeving mogelijk plaatsvinden met je stem, oogbewegingen en specifieke lichaamsbewegingen. Onderzoek laat zien dat hoewel gebruikers in VR fysiek ver van elkaar verwijderd zijn, de nabijheid van andere gebruikers in VR kan leiden tot het gevoel van intimidatie en aantasting van de persoonlijke ruimte.[8] De interactie wordt dus intiemer. Dit roept vragen op over fysieke integriteit in een digitale wereld. In december 2021 werd een vrouw in een testomgeving van Horizon Worlds (de VR-omgeving gebouwd door Meta) onwenselijk betast via haar avatar. Horizon Worlds had wel een zogenaamde 'safe zone'-tool die ervoor zou moeten zorgen dat je avatar niet aangeraakt kan worden, maar het voorbeeld laat zien dat virtuele werelden niet altijd veilig zijn.[9] Wie is uiteindelijk verantwoordelijk voor misstanden in een virtuele wereld en wie handhaaft gezamenlijke normen? Welke rol kan de politie hierin spelen?

Schadelijk gedrag in de metaverse

Mechanismen van het internet die kunnen leiden tot schadelijk gedrag online, zullen zich mogelijk herhalen in de metaverse. Voorbeelden van mechanismen zijn hyperconnectiviteit, viraliteit, anonimiteit online en onduidelijke omgangsnormen. Deze mechanismen kunnen schadelijk gedrag zoals intimidatie, de verspreiding van desinformatie, discriminatie en cyberbedrog in de hand werken. Het is aannemelijk dat deze mechanismen en gedragingen ook de metaverse zullen kenmerken als we niets doen om dit bij te sturen. Daarbij komt dat uitingen van haat, pesterij en geweld in de metaverse misschien nog wel harder aankomen dan op het huidige internet. Waar een stroom aan haatberichten op je Twitterlijn al enorm schadelijk kan zijn voor een individu, is het misschien nog intenser als je avatar wordt achtervolgd en uitgescholden door een groep boze avatars in een 3D-wereld. Wie wordt verantwoordelijk voor het reguleren van schadelijke content en welke rol hebben handhavende autoriteiten hierbij?

Cybercrime in de metaverse

Een risico waar de politie nu al mee geconfronteerd wordt, maar dat in de toekomst mogelijk nog meer aanwezig zal zijn, is de betrouwbaarheid van het gebruik van NFT's en blockchaintechnologieën. Denk hierbij aan mogelijke frauduleuze praktijken bij het gebruik van NFT's en economische zeepbellen in de cryptosector[10]. Daarnaast is het nog maar de vraag hoe veilig de blockchaintechnologie achter de beveiliging van NFT's zal blijken in de toekomst.[11] Cyberfraude is geen nieuw fenomeen, maar kan een hoge vlucht nemen in de metaverse. Hoe gaat de politie hiermee om bij de aanpak van fraude?

Andere maatschappelijke risico's zijn onder

meer de mogelijke milieu-impact van de metaverse en uitvergroting van sociale ongelijkheid omdat mogelijkerwijs niet iedereen makkelijk toegang zal kunnen krijgen tot de metaverse, onder andere omdat VR-headsets en toekomstige AR-brillen peperduur zijn.

Oproep tot dialoog

We zien de discussie over de gewenste inrichting van de metaverse vanuit maatschappelijk perspectief voorzichtig op gang komen. Maar deze ontwikkeling gaat iedereen in de samenleving aan, en daarom is een brede maatschappelijke discussie wenselijk. Want ongeacht of je de geschetste beelden over de metaverse realistisch acht of niet, gezien de enorme investeringen en marketing rond de metaverse is het haast onvermijdelijk dat deze er in een bepaalde verschijningsvorm gaat komen.

Het Rathenau Instituut heeft op basis van risico's als gevolg van toepassingen door immersieve technologieën tien ontwerpeisen opgesteld voor veilige technologieën voor een digitale samenleving van morgen. Zo willen we baas blijven over ons eigen digitale lijf, willen we controle behouden over onze virtuele identiteit en willen we bescherming tegen manipulatie en beïnvloeding. Deze ontwerpeisen willen we samen met belanghebbenden in de maatschappij uitwerken voor de metaverse. We zijn daarom ook benieuwd naar de rol die de politie voor zichzelf ziet. •

6 Zie www.rathenau.nl voor de rapporten 'Online Ontspoord', 'Verantwoord Virtueel', 'Nep Echt' en 'Hoor wie het zegt'.
7 Zie www.rathenau.nl
8 Snijders, D., Horsman, S., Kool, L., & Van Est, R. (2020). *Responsible VR. Protect consumers in virtual reality.* The Hague: Rathenau Instituut, p. 40.
9 Zie https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/
10 Stikker, M. (2022).
11 NRC (2021).

Wat is de metaverse?

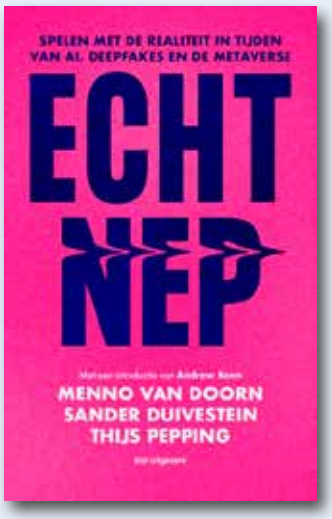
De metaverse wordt vaak vergeleken met Secondlife, een virtuele wereld die in 2002 werd opgericht. De droom vanuit de techwereld is echter dat we niet via een beeldscherm achter een toetsenbord inloggen in de metaverse, maar door middel van augmented reality (AR)[1] en virtual reality (VR)[2]. Er bestaan verschillende ideeën over wat de metaverse is of zou kunnen zijn. In de media, op online fora en in wetenschappelijke tijdschriften komen we grofweg drie benaderingen tegen. Sommigen beschrijven de metaverse als een virtuele omgeving waarin het online en het echte leven steeds meer verweven raken (1); anderen zien de metaverse vooral als een volgende stap in het creëren van een virtuele economie (2); en ten slotte beschrijven met name onderzoekers de metaverse als sociaal-digitale infrastructuur (3). De drie benaderingen sluiten elkaar overigens niet uit.

1 Augmented reality (AR) is een digitale techniek die met behulp van een AR-bril of een telefoon of tablet een extra digitale laag over de werkelijkheid legt.
2 Virtual reality (VR) is een digitale techniek die je met hulp van een VR-bril naar een andere werkelijkheid transporteert. Wie een VR-bril opzet, waant zich in een geheel andere wereld die een sterke, fysieke sensatie teweeg kan brengen.

Recensies over actuele publicaties

BOEK

Echt nep



Geen luchtig leesvoer, maar gelukkig wordt de driehonderd pagina's tellende uiteenzetting door middel van vier 'Google'-vragen in behapbare stukken gehakt

Recensent dr. **Maud van Bavel** is onderzoeker bij Politie Nederland.

M. van Doorn, S. Duivestein & T. Pepping (2021). *Echt nep. Spelen met de realiteit in tijden van AI, deepfakes en de metaverse,* Bot uitgevers, Voorschoten, 312 pagina's, ISBN 9789083069692

Echt nep, een boek over 'online nepperij' geschreven door drie techno-futuristen uit Nederland, schetst een soms verontrustend maar vooral optimistisch beeld van de nabije toekomst. Door in gesprek te gaan met filosofen, gedragswetenschappers en andere experts wordt verder gekeken dan de bekende doemscenario's die we uit sciencefictionfilms kennen. Het is geen luchtig leesvoer, maar gelukkig wordt de driehonderd pagina's tellende uiteenzetting door middel van vier 'Google'-vragen in behapbare stukken gehakt:

- Vraag 1: Beste Google, verdwijnt het verschil tussen 'echt' en 'nep'?
- Vraag 2: Beste Google, waarom verliezen feiten het zo vaak van fictie?
- Vraag 3: Beste Google, hoe worden synthetische media gebruikt om nieuwe verhalen te vertellen?
- Vraag 4: Beste Google, hoe herstellen we onze relatie met de realiteit?

Technologie, zo stellen de auteurs, verandert onze relatie met de werkelijkheid. Er wordt gespeeld met de realiteit. Wat is nog écht? En wat is wenselijk?
Uiteenlopende gradaties aan 'nep' content worden uiteengezet, van onschuldig en grappig tot zeer schadelijk. Verschillende onderwerpen passeren de revue, zoals het verschil tussen misinformatie en desinformatie, de voor- en nadelen van *deep fakes*, het bestaan van digitale mensen en de (vaak onderschatte) kracht van *memes*. Er is zelfs een *shout-out* naar jeugdagent Kim van de Amsterdamse politie, in een paragraaf over synthetische verhalenvertellers.
Synthetisch betekent: kunstmatig gemaakt. Volgens de auteurs zijn synthetische media strikt genomen *door kunstmatige intelligentie gemanipuleerde of gecreëerde data en media.* Dat klinkt wellicht als een futuristische ver-van-je-bed-show, maar is alom aanwezig: de filters op Snapchat of in MS Teams, bijvoorbeeld, waarin we de visuele achtergrond tijdens een online vergadering kunnen aanpassen. Ook Hollywood maakt er gretig gebruik van: in de populaire serie 'The Mandalorian' zijn zowel deepfake als AI-technologieën toegepast. En de toolkit blijft zich uitbreiden.
Met de opkomst van synthetische media bevinden we ons volgens de auteurs nu in de vierde mediarevolutie. De eerste revolutie beslaat de analoge (zetletters en boekdrukpers), de tweede de elektronische (radio en televisie), de derde de digitale (web en mobiel), en nu dus een type media waarvoor geautomatiseerde creatie en manipulatie de kern vormen. Oftewel: tegenwoordig kan iedereen met behulp van kunstmatige intelligentie creatief aan de slag met beeld en geluid. En deze resultaten worden steeds moeilijker van het 'echte' origineel te onderscheiden. Inmiddels wordt zelfs het begin van een vijfde revolutie gesignaleerd, die draait om cryptomedia.
Dat fictie sterker is dan feiten, komt onder meer naar voren in een hoofdstuk over 'conspiritualiteit', waarin de rol van synthetische media in het ontstaan en verspreiden van complottheorieën wordt belicht. In het daaropvolgende deel rolt het complotballetje verder en wordt de oorsprong van een aantal bekende samenzweringstheorieën verklaard, waaronder Wayfairgate (dat nog een Nederlands staartje kreeg met artiest Lange Frans en bol.com). Er is ook goed nieuws wat betreft de gigantische hoeveelheid complottheorieën: des te meer stromingen, des te kleiner de kans dat er één dominant wordt.
Deze ontwikkelingen hebben ook gevolgen voor de economie. Veel geld, producten en diensten zijn tegenwoordig virtueel: denk hierbij aan de handel in digitale objecten, zoals bitcoins en NFT's. En uiteindelijk kan de overgang van echt naar nep leiden tot het zogeheten 'metaverse', waar fysiek en virtueel elkaar overlappen.
Het boek sluit af met een filosofische maar positieve noot dankzij een aantal motiverende herstelverhalen. De auteurs pleiten voor een nieuwe realiteitsethiek, onderstrepen de verantwoordelijkheid van bigtechbedrijven en de vele kansen voor digitaal geluk en welzijn.
De wirwar aan technologische innovaties, nieuwe termen en internettrends: het duizelt je af en toe als lezer. Maar *Echt nep* is bovenal leerzaam en stemt voorzichtig hoopvol.

BOEK

Het kan ook nooit normaal

L. Hester (2022). *Het kan ook nooit normaal. Belevenissen van een hoofdagent*, Harper Collins, Amsterdam, 320 pagina's € 21,99, ISBN 9789402709674

Ze was één van de collega's die gevolgd werden bij hun werk in het televisieprogramma *Bureau Burgwallen*, maar ze vlogt ook over haar werk en schreef er een boek over. Aan de hand van een reeks verhalen over wat zij meemaakt als politieagente geeft deze ras-Amsterdamse in een hele persoonlijke beleving het politiewerk in voornamelijk de incidentafhandeling weer. Ik zette het op mijn e-reader en heb het in één ruk uitgelezen. Omdat ik er veel in herken, maar ook omdat ik het eigen verhaal van een collega een hele fijne afwisseling vind naast alles wat er door anderen over de politie wordt geschreven.

Wat het boek bijzonder maakt, is de mate van detail in de beschrijving en vooral van de eigen beleving en emotie. Zo wordt bijvoorbeeld een melding huiselijk geweld beschreven, waarin Lieke en haar collega een zwaar mishandelde en van al haar vrijheden beroofde vrouw aantreffen. Na enige overreding besluit de vrouw haar man te verlaten en Lieke en haar collega helpen haar een koffer te pakken. De vrouw is doodsbang dat haar echtgenoot ondertussen thuiskomt. Lieke: "Ik schijt zeven kleuren stront bij het idee dat die klootzak van een man van haar zo voor de deur staat. Niet dat ik bang ben dat Sander en ik hem niet aankunnen, maar ik vrees wel dat Samira's toch al weinige kracht als sneeuw voor de zon verdwijnt op het moment dat ze hem ziet."

Lieke houdt van de chaos en drukte in de binnenstad en dat beschrijft ze dan ook in geuren en kleuren. Ze laat zien dat politiewerk mensenwerk is. Sympathiek is haar compassie voor kwetsbare mensen. Zo start het boek met een brief aan potentiële zelfmoordplegers: bel 112. Leuk is ook het verhaal over de oude dame die dacht dat haar fiets gestolen was, maar zich door Lieke geholpen herinnert dat haar dochter de fiets had uitgeleend. Verder zijn er beeldende observaties over daklozen, zoals tijdens de coronalockdown, "hoe het opeens opvalt dat er zo veel daklozen zijn. Als iedereen thuis zit, blijven de mensen die niet naar huis kunnen over. En dat zijn er veel. Heel veel."

Deze stoere en kundige politievrouw blijkt zelf ook kwetsbaar. Het aanspreken van een groep dronken mannen eindigt in geweld tegen haar collega en haarzelf met een hele lang nasleep. De mannen beginnen op haar in te slaan "Fuck, fuck, fuck, dit zijn geen gewone vuisten, besef ik direct. Ik krijg klappen met een voorwerp... We zijn in levensgevaar..." Lieke beschrijft hoe haar waarneming vertraagt, haar collega haar uiteindelijk ontzet en hoe blij ze is als de hulptroepen arriveren. "Mijn blauwe familie is hier, om te helpen." Wat volgt is een zware hersenschudding, bijna drie jaar revalidatie en tot haar grote smart enige tijd een zeker onvermogen om te kunnen gaan met chaos en drukte waar ze juist zo van houdt. Ze beschrijft de frustratie en teleurstelling over slechts taakstraffen voor twee van de vier daders. Meer weten en haar slachtofferverklaring lezen? Lees het boek!

De auteur laat zien dat **politiewerk mensenwerk** is

Recensent dr. mr. **Barbara van Caem** is hoofd van de cluster wetenschap bij de Landelijke Portefeuille Gebiedsgebonden Politie.

De valse belofte van evidence-based policing

REACTIE OP ARTIKEL VAN STIJN RUITER EN RONALD VAN STEDEN

In het januarinummer van het *Tijdschrift voor de Politie* schreven Stijn Ruiter en Ronald van Steden een artikel over evidence-based policing: *Politiewerk met bewijskracht*.[1] Evidence-based policing is als term geïntroduceerd door de Amerikaanse politieonderzoeker Lawrence Sherman: politiewerk zou gebaseerd moeten zijn op wat bewezen het meest effectief is, op *what works*. Het heeft vooral navolging gevonden in het Verenigd Koninkrijk en de Verenigde Staten.

Over de auteur
Prof. dr. Otto M.J. Adang is lector Openbare orde & Gevaarbeheersing aan de Politieacademie en bijzonder hoogleraar Veiligheid en collectief gedrag aan de faculteit Gedrags- en Maatschappijwetenschappen van de Rijksuniversiteit Groningen.

Zoals de auteurs constateren, heeft het in Nederland nog geen hoge vlucht genomen en daar willen ze graag verandering in brengen. Want: "Door te kiezen voor een wetenschappelijk onderbouwde werkwijze kan politiewerk worden verbeterd, kunnen mogelijk kosten worden bespaard en kunnen niet of zelfs averechts werkende interventies worden voorkomen." Wie wil dat nou niet? Als politieonderzoeker wil ik zelf ook graag naar wetenschappelijk onderbouwde interventies. Toch is er wat mij betreft sprake van een valse belofte van de evidence-based policing benadering. Hoe zit dat?

Het probleem is dat Sherman en zijn navolgers een beperkte zienswijze hebben op wat geldt als 'evidence'. De evidence-based benadering hanteert een strenge hiërarchie in de mate waarin verschillende onderzoekdesigns bewijs leveren voor de effectiviteit van interventies, de Maryland Scale of Scientific Methods. Bovenaan de hiërarchie staat het experiment, gerandomiseerd en met controlegroepen. Adepten van de evidence-based benadering erkennen weliswaar (en Ruiter en Van Steeden doen dat ook) dat het ideale niet altijd haalbaar is en dat al het onderzoek dat bijdraagt aan het verstevigen van de bewijskracht waardevol is. Tegelijkertijd: andere onderzoeksmethoden staan per definitie toch minder hoog aangeschreven in de evidence-based benadering, en publicaties die niet voldoen aan die 'goudstandaard' worden minder serieus genomen en vaak ook niet meegenomen in literatuurreviews.

Randomized controlled trials

Ruiter en Van Steden stellen dat er allerlei prachtige voorbeelden zijn van randomized controlled trials naar politiewerk, maar noemen geen concreet voorbeeld. In een online gepubliceerd *factsheet*[2] deed Ruiter dat onlangs wel. Hij verwijst naar een Engels onderzoek naar de invoering van het stroomstootwapen bij de City of London Police (Ariel et al., 2018[3]) die op basis van een randomized controlled

onderzoeksdesign concluderen dat de aanwezigheid van het stroomstootwapen in situaties causaal samenhangt met meer geweldsgebruik door agenten en meer geweldspleging tegen agenten. Zonder bewijs van het tegendeel, stelt Ruiter, moet er rekening mee worden gehouden dat de genoemde negatieve effecten zich niet beperken tot Londen. Voor Ruiter is dit 'gedegen' onderzoek een schoolvoorbeeld van de waarde van de evidence-based policing, voor mij is het een schoolvoorbeeld van de valse belofte ervan. In wat volgt zal ik uitleggen waarom en waarom dit onderzoek dezelfde manco's heeft als veel ander onderzoek in de evidence-based benadering.

Het stroomstootwapen

Om te beginnen is het handig om na te gaan of het wel klopt wat de Engelse onderzoekers concluderen. Ze hebben zeker keurig volgens de regelen der kunst een Randomized Control experiment opgezet, waarbij ze een jaar lang gegevens verzamelden bij de London City Police. In de onderzoeksperiode is negenmaal het stroomstootwapen getrokken, waarbij ook tweemaal daadwerkelijk de pijltjes zijn afgevuurd. Dat is niet zoveel in een jaar tijd, maar daar ging het de onderzoekers ook niet om. Zij hadden een hypothese, namelijk dat de zichtbare beschikbaarheid van stoomstootwapens een causale factor is die de kans dat verdachten agressief gedrag vertonen naar agenten vergroot.

Die hypothese is niet gebaseerd op literatuur over stroomstootwapens of ervaringen uit de praktijk. Integendeel, ervaringen uit de praktijk (in Engeland, in Nederland en elders) wijzen erop dat het tonen van het stroomstootwapen of het ermee dreigen vaak voldoende is om medewerking van verdachten te verkrijgen.[4] De hypothese van de onderzoekers is gebaseerd op het zogenaamde 'wapeneffect': een vrij robuuste

> Adepten van de evidence-based benadering **erkennen** dat het ideale **niet altijd haalbaar** is

bevinding uit de literatuur dat de zichtbare aanwezigheid van *vuurwapens* leidt tot een toename in agressief gedrag. Maar… die literatuur over het '(vuur)wapeneffect' is volledig gebaseerd op experimenten onder laboratoriumomstandigheden. Geen enkele van die experimenten heeft betrekking op de interactie tussen politie en burgers. Er is tot nu geen enkele reden om aan te nemen dat het feit dat agenten standaard geweldsmiddelen bij zich dragen op zich leidt tot agressie in hun richting. Toch veronderstellen de auteurs dat er ook sprake is van een 'less-than-lethal-wapens effect'. En dat vinden ze dan vervolgens ook: er is sprake van een verdubbeling (van 3 naar 6) van 'aanvallen' op agenten met stroomstootwapens vergeleken met agenten zonder stroomstootwapen in de onderzoeksperiode. Die getallen zijn klein, maar volgens de analyse van de onderzoekers toch statistisch significant. In hoeverre een dergelijke toename ook betekenisvol is, is wat mij betreft de vraag. Bovendien zijn er ook andere verklaringen denkbaar voor deze verdubbeling. Misschien gedragen agenten die met een stroomstootwapen bewapend zijn zich anders dan agenten zonder stroomstootwapen? De auteurs leggen niet uit waarom agenten immuun zouden zijn voor het wapeneffect met betrekking tot de wapens die ze zelf dragen. Zijn ze bijvoorbeeld minder terughoudend? Hebben ze meer zelfvertrouwen om handhavend op te treden? Die verklaring sluiten de auteurs uit, ondanks het feit dat ze ook meer geweldgebruik zien bij de agenten met het stroomstootwapen (48% meer, ze geven geen absolute aantallen). Want, zeggen de auteurs, er zijn niet meer klachten of verwondingen vergeleken met de controlegroep en de literatuur zegt ook dat agressie meestal van de kant van verdachten komt en niet van agenten… Dus, stellen ze, *the*

1 Ruiter, S. & Van Steden, R. (2022). Politiewerk met bewijskracht. *Tijdschrift voor de Politie, 1*, 6-10
2 https://nscr.nl/factsheet/de-invoering-van-het-stroomstootwapen-hoe-zit-het-met-de-evidence-base/ en https://nscr.nl/app/uploads/2022/01/NSCR_Factsheet_Pilotstudies-Stroomstootwapen_280122.pdf
3 Ariel, B., Lawes, D., Weinborn, C., Henry, R., Chen, K., & Brants Sabo, H. (2018). The "Less-Than-Lethal Weapons Effect"—Introducing TASERs to Routine Police Operations in England and Wales: A Randomized Controlled Trial. *Criminal Justice and Behaviour 46*(2): 280-300 DOI: 10.1177/0093854818812918
4 Adang, Mali & Vermeulen (2022). *Geweldig of gevaarlijk? Het stroomstootwapen in de basispolitiezorg.* Boom Criminologie, Den Haag

> Verschillende situaties **lijken** misschien **op elkaar**, maar zijn toch ook weer in veel opzichten **anders**

presence of a TASER precipitates a pattern where suspects become more aggressive toward officers, who in turn retort with more forceful responses, and not vice versa.

Dat is, los van de beperkte aantallen, toch wat kort door de bocht. Het is bijvoorbeeld niet bekend of het effect blijvend is, of misschien alleen optreedt kort na introductie van het stroomstootwapen. Het stroomstootwapen was wel erg prominent zichtbaar en agenten die een stroomstootwapen droegen, zagen er ook anderszins nogal anders uit dan hun collega's zonder stroomstootwapen (zie foto in deze bijdrage[5]), zodat niet geconcludeerd kan worden dat de zichtbare aanwezigheid van het stroomstootwapen de variabele was die het verschil veroorzaakte.

Zijn er dus bij de bevindingen van het onderzoek al grote vraagtekens te plaatsen, de problemen worden nog groter als je de conclusies wilt vertalen naar andere korpsen en andere landen, zoals Ruiter doet. De London of City Police is namelijk nogal een uitzonderlijk politiekorps, zoals het op de eigen website ook vermeldt: *policing the square mile brings with it particular challenges, unlike any other policing area in the UK*.[6] De vierkante mijl die het werkterrein van de City of London police is, kent slechts zo'n tienduizend inwoners. De City bestaat grotendeels uit kantoren. Het aantal slachtoffergerelateerde delicten is er zesmaal zo laag als in de rest van Engeland & Wales (0,1 per persoon t.o.v. 0,6 per persoon). Generaliseerbaar naar een land als Nederland, waar agenten standaard bewapend zijn met een vuurwapen, zijn de resultaten in elk geval niet. Zoals de auteurs zelf aangeven: *the presence of a firearm will probably overshadow or interact with the effect of the presence of a TASER*. Daarnaast is de draagwijze van het stroomstootwapen in Nederland totaal anders: in plaats van prominent midden op de borst (zie foto) dragen Nederlandse agenten het stroomstootwapen minder nadrukkelijk zichtbaar, namelijk op het bovenbeen. Het duidt op een probleem dat voorstanders van evidence-based policing onderzoek ook wel kennen: *situational and contextual factors are critical to understanding the mechanisms of TASER effects*, schrijven de

5 Bron: tweet @CityPolice https://pbs.twimg.com/media/DY_n70nX4AYfSOX.jpg:large

6 https://www.cityoflondon.police.uk/police-forces/city-of-london-police/areas/city-of-london/about-us/about-us/

auteurs (hetzelfde geldt voor de effecten van iedere politie-interventie[7]). In een voetnoot voegen de auteurs daar nog aan toe:

> "We note that our outcomes did not look at the efficacy of TASER or its necessity more broadly. The stack of evidence on the availability of TASERs, as reviewed earlier, tends to suggest prominent benefits for law enforcement. Our findings do not suggest otherwise. Our recommendations, therefore, suggest ways to improve rather than to reduce the deployment of TASERs in policing."

Wankele basis

De bevindingen van het onderzoek van Ariel et al. zijn daarmee op geen enkele manier in tegenspraak met de bevindingen van het onderzoek naar de Nederlandse pilot met het stroomstootwapen. Hun conclusie dat het stroomstootwapen leidt tot meer agressie van verdachten, is aanvechtbaar en hoe dan ook, vanwege de onvergelijkbaarheid, irrelevant voor de Nederlandse situatie. Nadere beschouwing van het onderzoek van Ariel et al. legt genadeloos de beperkingen van de evidence-based benadering bloot. De focus op de (superieur geachte) methode van het gerandomiseerde experiment gaat voorbij aan de evidente zwakke punten van het onderzoek. Sommige van die zwakke punten zijn specifiek voor het onderzoek (de wankele basis voor het veronderstellen van een less-than-lethal wapen effect), andere zijn karakteristiek voor de evidence-based benadering en de moeilijkheid om in praktijkomstandigheden een goed experiment uit te voeren. Een experiment vereist een vraagstelling die zich beperkt tot een enkele variabele, waardoor noodgedwongen de conclusies ook beperkt zijn en tot bescheidenheid zouden moeten leiden. In de praktijk van het politiewerk is er echter sprake van een groot aantal elkaar wederzijds beïnvloedende afhankelijke en onafhankelijke variabelen. Een zuivere experimentele benadering van de wijze waarop de politie daadwerkelijk optreedt in gevaarsituaties (of andere interventies doet) is nagenoeg onmogelijk. Uitschakeling van alle interveniërende variabelen is niet realistisch. Verschillende situaties lijken misschien op elkaar, maar zijn toch ook weer in veel opzichten anders. De operationele context laat zich niet weg-organiseren. De onderzoekers in het Engelse onderzoek liepen daar ook tegenaan, toen een periode van terrorismedreiging de experimentele opzet verstoorde. Hoe strakker je het experiment opzet, gericht op een factor, met uitsluiting van anderen om een goede controlegroep mogelijk te maken, hoe problematischer het is om de bevindingen te generaliseren. Context is alles in politieonderzoek.

> De **resultaten** van de evidence-based benadering zijn **niet of nauwelijks generaliseerbaar**

Daarom is de belofte van de evidence-based benadering vals: de resultaten zijn niet of nauwelijks generaliseerbaar. En bij het interpreteren van de resultaten van politieonderzoek is goede kennis van de politiepraktijk onontbeerlijk. Daar ontbreekt het nogal eens aan. De evidence-based adepten (Ruiter & Van Steden incluis) erkennen noodgedwongen het belang van context wel, maar claimen ten onrechte toch hun plaats aan de top van de bewijshiërarchie.

Reflecteren op de praktijk

Zoals Wood et al. (2018) ook stellen in een paper dat wat mij betreft verplichte literatuur zou moeten zijn voor iedere politieonderzoeker: de evidence-based benadering leidt tot *exaggerated claims* over wat gekend kan worden over politiewerk. Politiewerk is extreem contextafhankelijk en het zou beter zijn om te spreken over wat werkt in een specifieke context. Wood et al. voegen daar nog iets belangrijks aan toe: "Kennis en bevindingen over politiewerk zijn geen abstracties, maar krijgen betekenis door *cognitive agents*: politiemensen die, hopelijk samen met politieonderzoekers, kritisch reflecteren op hun praktijk." Daar ligt een belangrijk rol voor politiewetenschappers, en dat wordt niet geholpen door een eenzijdige en onjuiste claim op wat 'bewijs' is, en wat wel of niet mee mag tellen als waardevolle kennis.

7 Zie Wood, D., T. Cockcroft, S. Tong & R. Bryant (2018) The importance of context and cognitive agency in developing police knowledge: Going beyond the police science discourse. The Police Journal: Theory, Practice and Principles 91(2) 173–187

Politieacademie
Police Academy of the Netherlands

GESLAAGD

Aan de Politieacademie studeren jaarlijks vele politiefunctionarissen af. Voor deze rubriek selecteren de opleiders van de Politieacademie enkele boeiende en goed beoordeelde verslagen van afstudeeronderzoeken. De meeste scripties kunnen bij de Mediatheek van de Politieacademie (www.politieacademie.nl/mediatheek) geraadpleegd worden. Publicatie aldaar is afhankelijk van de rubricering van de mate van vertrouwelijkheid. De scripties van onderstaande studenten kunt u rechtstreeks aanvragen via het vermelde e-mailadres.

Van samen werken naar samenwerken

Een studie naar discontinuïteit in de samenwerking tussen de actoren van het begeleidingsteam

Carina van Diepenbos, carina.van.diepenbos@politie.nl
Thesis Politiekundige

Hoe slagen verschillende teams erin om vanuit meerdere perspectieven en invalshoeken tot een samenwerking te komen? Om hier achter te komen is er een onderzoek uitgevoerd dat zich richt op de mate van discontinuïteit die de actoren uit het begeleidingsteam in de samenwerking ervaren.

Het uitgangspunt van PO21 is dat het begeleidingsteam samenwerkt om de student zo optimaal mogelijk tijdens zijn leerproces te faciliteren. De verschillende actoren slaan een brug vanuit hun eigen praktijk en belangen naar een gemeenschappelijke werkomgeving en visie om de student startbekwaam te maken. Uit eerder onderzoek (Buijs & Nieuwenhuis, 2021) blijkt echter dat aspiranten zich kritisch hebben geuit over de samenwerking tussen de Politieacademie en de eenheden. Docent Politieacademie Amsterdam: "Ik kan niet zeggen dat er al een samenwerking is. Het is meer het contact hebben over de student."

Dit onderzoek resulteert in praktische aanbevelingen om de continuïteit in de samenwerking te herstellen/waarborgen.

Zicht op criminele spookbewoning

Gert Vuik, gert.vuik@politie.nl
Thesis Politiekundige

Spookbewoning leidt tot leefbaarheids- en veiligheidsproblemen, het zorgt voor maatschappelijke druk op de woningmarkt door de verminderde beschikbaarheid van huurwoningen en (illegale) bewoners. Bewoners die veelal ook slachtoffer zijn van uitbuiting of het verkeren in een (gevoelsmatige) afhankelijkheidsrelatie.

Deze combinatie maakt dat vele (maatschappelijke) actoren bij spookbewoning betrokken zijn, wat leidt tot een complex vraagstuk op het gebied van toezicht, controle en handhaving. Spookbewoning kan een goede indicator zijn dat het pand een faciliterende functie heeft bij georganiseerde criminaliteit. De term criminele spookbewoning is gekozen voor de combinatie van criminaliteitsvormen met spookbewoning en/of oneigenlijk gebruik.

De scriptie bevat een viertal onderdelen. Ten eerste de signalen van criminele spookbewoning, ten tweede waarom het kan blijven voortbestaan door de (on)mogelijkheden van informatiedeling tussen politie en gemeente, ten derde hoe het huidige registratiesysteem BVH voorkomt dat het onderwerp urgentie krijgt en tot slot hoe een basisteam van de politie zijn informatiepositie zou kunnen inrichten richting interne en externe partners.

Aanbevelingen zijn om:

- de gegevensdeling tussen politie en gemeente (en gemeentelijke afdelingen onderling) over concrete adressen en personen rond criminele spookbewoning praktisch eenvoudig maar op een rechtmatige manier mogelijk te maken. De hoeveelheid convenanten kan dan vervallen.
- het politieregistratiesysteem anders in te richten met één hoofdregistratiecode (bijvoorbeeld ondermijning) met daaronder diverse subcodes zoals spookbewoning.

Tekst: Teun-Pieter de Snoo, Politieacademie & Jan van Balkom

Jelle Janssens, Wim Broer, Mark Crispel & Renze Salet (eds.)

Informatiegestuurde politie

Cahiers Politiestudies, nr. 54

In het streven het politiewerk gerichter, effectiever en efficiënter te maken door een degelijke analyse van beschikbare informatie, wordt het ideaal van een 'informatiegestuurde politie' al enkele decennia nagestreefd in vele politieorganisaties. Het omzetten van dit ideaal naar de praktijk gaat echter niet zonder slag of stoot. De Parlementaire Onderzoekscommissie Terroristische Aanslagen in België toont aan dat de informatiepositie van de Belgische geïntegreerde politie niet optimaal is. In Nederland werd anderzijds het 'Criminaliteits Anticipatie Systeem' (CAS) landelijk geïmplementeerd. Geavanceerde plannings- en voorspellingsmethoden helpen te voorspellen welke incidenten waar zullen plaatsvinden. De technologische omgeving waarin de politie functioneert, is grondig gewijzigd. De mogelijkheden om grote hoeveelheden 'big data' op te slaan en te analyseren zijn enorm toegenomen. Deze ontwikkeling werpt de vraag op in hoeverre het lukt om de politie om te vormen tot een hoogwaardige informatie- en kennisorganisatie.

Welke beperkingen en voorwaarden doen zich daarbij voor? Hoe krijgen noties als 'predictive policing' of 'policing of risks' in de praktijk vorm? Wat zijn de morele en normatieve aspecten en vragen die deze ontwikkelingen bij de politie oproepen?

Frans Osinga (voorzitter), Wilbert Jan Derksen (scribent), Tamara de Bel, Dennis Broeders, Paul Ducheine, Marijn Janssen, Sander Klous & Ronald Prins

Digitalisering en liberale kernwaarden

Vrijheid door grenzen te stellen in de digitale wereld

TeldersStichting Geschriften, nr. 132

Digitalisering heeft een fundamentele impact op de samenleving. In een relatief kort tijdsbestek zijn zaken als het internet, de smartphone en sociale media een grote rol gaan spelen in ons dagelijks leven. Het opzoeken van informatie is makkelijker dan ooit en langs digitale weg kunnen we moeiteloos met elkaar communiceren. Ook binnen sectoren als het onderwijs en de gezondheidszorg zijn toepassingen van digitale technologie niet meer weg te denken. Het is evident dat digitalisering aldus een verrijking is gebleken voor mens en maatschappij. Desalniettemin zijn er ook belangrijke problemen op het gebied van digitalisering te noemen die vragen oproepen.

Hoe beteugelen we de datazucht van grote techbedrijven? Op welke manier kunnen we het schadelijke effect van desinformatie minimaliseren? Wat kunnen we doen tegen het gebruik van discriminerende algoritmen door de overheid? Hoe beschermen we onszelf tegen cyberaanvallen?

In dit geschrift wordt vanuit een liberaal perspectief gereflecteerd op de belangrijkste uitdagingen die digitalisering oplevert ten aanzien van de vrije markt, de democratie, de relatie tussen burger en overheid, en de veiligheid van de samenleving. Ook wordt er gekeken hoe het digitaliseringsbeleid kan worden ingebed in een algemene governance-strategie. In deze publicatie wordt op toegankelijke wijze duidelijk gemaakt dat de vraagstukken rond digitalisering voor iedereen relevant zijn en dat het tijd is voor de politiek om tot actie over te gaan.

Bestel nu op www.gompel-svacina.eu

Gompel&Svacina

PELI™ BUILT TO PROTECT

DÉ STANDAARD IN VEILIGHEID

VONK

Voorstraat 41 | 3265 BT Piershil | +31 (0)88-03 3030 0 | info@vonkbv.com | www.vonkbv.com