

NAVIGEREN IN NIEMANDSLAND

ZEVEN URGENTE UITDAGINGEN RONDOM
DIGITALISERING EN AI IN POLITIEWERK

Navigeren in niemandsland

Zeven urgente uitdagingen rondom
digitalisering en AI in politiewerk

Advies 02 WARP – juni 2025



Inhoud

Ten geleide	3
Navigeren in niemandsland	5
Tot slot	22
Referenties	23
Eindnoten	25
Bijlage I – Deeladvies Instellen evaluatiecommissie	
Wet politiegegevens	29

Ten geleide

Navigeren in niemandsland is een advies van de Wetenschappelijke Adviesraad Politie (WARP). In algemene zin is de opdracht aan de Raad als volgt (Instellingsbesluit, artikel 2.4):

De Wetenschappelijke Adviesraad Politie heeft tot taak de korpschef gevraagd en ongevraagd vanuit wetenschappelijke inzichten te adviseren en duiding te geven met betrekking tot de politiefunctie, het functioneren van de politie en op het gebied van maatschappelijke vraagstukken die in relatie staan tot het functioneren van de politie binnen de samenleving.

De nadruk ligt daarbij op brede vraagstukken met betekenis voor de langere termijn. In het formuleren van zijn adviezen kiest de Raad voor een multidisciplinaire benadering, hetgeen tevens wordt weerspiegeld in de samenstelling van de raad.

Dit advies is voorbereid door een interne projectgroep van de Raad. Deze bestond uit de raadsleden prof.dr.mr. Marc Schuilenburg en prof. dr. Ellen Giebels, en de adviseurs dr. Auke van Dijk, Mijchanou Kowalczyk MA, Olga Akhrarova MSc, met medewerking van dr. Wendy Schreurs (Politieacademie). Het in Bijlage I opgenomen deeladvies is voorbereid door de raadsleden (tot 1 juni 2024) prof.dr. Bart Jacobs en prof.dr.mr. Lonneke Stevens, en adviseur dr. Patty de Bruine. De Raad is de voormalig leden Jacobs en Stevens erkentelijk voor de toestemming het deeladvies als onderdeel van dit bredere advies uit te brengen.

In het adviestraject is in de vorm van een interview of expertmeeting gesproken met de volgende met naam te noemen experts.

David Davidson MSc (Follow the Money), Geert-Jan Staal (Politie), Jeroen van Rest MSc (TNO), drs. Katinka Knops (adviseur), prof.dr. Maaïke Endedijk (Universiteit Twente), prof.dr.ir. Maarten van Steen (Universiteit Twente), Michael Bots MSc (Politieacademie), Puck van de Ven MSc (Politie academie), Reinder Doeleman MSc EMIM (Politie), Remco van den Hoven BBA (Politie), dr. Wouter Landman (onderzoeker).

De Raad bedankt de respondenten voor hun bereidheid expertise te delen en met de werkgroep van gedachten te wisselen.

Navigeren in niemandsland

Aanleiding

Technologische ontwikkelingen op het gebied van dataverzameling en de toepassing van *Artificial Intelligence* (AI) en *Machine Learning* (ML) gaan razendsnel. Dit leidt tot grote uitdagingen in het politiewerk. Deze uitdagingen komen voort uit een spanningsveld tussen publieke waarden.¹ Enerzijds betreft het de goede invulling van publieke waarden zoals non-discriminatie, *accountability* (met menselijke tussenkomst) en het recht op privacy van burgers. Anderzijds zijn er kansen voor de opsporing van criminaliteit (veiligheid), het verbeteren van de relatie en communicatie met burgers (vertrouwen) en het stroomlijnen van werkprocessen (efficiency). Ook dit zijn belangrijke publieke waarden. Het advies 'Navigeren in niemandsland' identificeert zeven urgente uitdagingen voor de Nederlandse politie als het gaat om de inbedding en toepassing van data en AI.

Historie van datagebruik

Van oudsher spelen data een centrale rol in het politiewerk. Dit voert terug tot de 19e eeuw toen fotoarchieven van gezichten (mug shots) en vingerafdrukken van personen (dactyloscopie) werden aangelegd om bij te houden wie in aanraking was gekomen met de politie. Vanaf de jaren '80 en '90 van de 20e eeuw krijgt het verzamelen en verwerken van data een sterke impuls. Automatisering en informatisering via digitalisering zorgen ervoor dat steeds meer informatie wordt opgeslagen en interne werkprocessen worden gestandaardiseerd. Deze ontwikkelingen worden verder gevoed door de opkomst van het risico-denken, waarbij het werk van de politie steeds meer draait om het opbouwen van een optimale informatiepositie.² Strategieën binnen de politie die hierbij aansluiten zijn *hot spots policing*, waarbij politieactiviteiten gericht worden ingezet op de plaatsen waar criminaliteit zich concentreert, en *intelligence led policing*. Hierbij worden op basis van geanalyseerde informatie en kennis beslissingen genomen om beter te anticiperen ('proactief') op bepaalde vormen van criminaliteit.³ Aan het begin van de 21e eeuw worden de gevolgen van de digitalisering van de samenleving voor het politiewerk steeds duidelijker; van de toename

in aard en omvang van cybercriminaliteit tot een uitbouw van het klassieke fysiek waken naar het virtueel waken over veiligheid.

AI als een disruptieve kracht

De meest recente technologische ontwikkeling is de integratie van AI in het politiewerk, waarbij zelflerende algoritmen autonoom een weg zoeken door grote databestanden en daarbij op zoek gaan naar relevante patronen. De *High-Level Expert Group on Artificial Intelligence* van de Europese Commissie definieert AI als ‘systemen die intelligent gedrag vertonen door hun omgeving te analyseren en – met enige graad van autonomie – actie te ondernemen om specifieke doelen te bereiken’ (2019; zie ook art. 3 lid 1 AI Act). Het gaat hierbij om complexe toepassingen, in het bijzonder om applicaties die de mogelijkheid hebben om zelfstandig te leren en beslissingen te nemen. De komst van dit type AI is een volgende transformatie van het politiewerk, waarbij AI door én voorbij de hiervoor genoemde processen van automatisering en informatisering via digitalisering gaat.⁴ De Wetenschappelijke Raad voor het Regeringsbeleid⁵ spreekt in dit verband van een ‘systeemtechnologie’ en waarschuwt dat het zeer lastig is vooraf te bepalen welke publieke waarden hierdoor worden geraakt en op welke wijze: ‘dat zal op manieren gebeuren die we nu grotendeels nog niet kunnen voorzien’.

Voorspellen is lastig; anticiperen is noodzakelijk

Politiewerk wordt in toenemende mate gestuurd door data en de vraag is wat de nieuwe context betekent voor de uitvoering en inrichting van het politiewerk.⁶ Deze vraag is relevant omdat politiemensen die met data en AI-toepassingen (gaan) werken met nieuwe uitdagingen worden geconfronteerd en deze uitdagingen een beroep doen op andere vermogens.⁷ Zo kunnen criminelen steeds gemakkelijker identiteiten stelen en misbruiken met behulp van *deepfake*- en *voice-cloning*-technologie (‘AI-criminaliteit’) en wordt het in bredere zin steeds lastiger het waarheidsgehalte van informatie in te schatten.⁸ Deze veranderingen raken aan fundamentele uitgangspunten voor de politieorganisatie.⁹ Niet alleen verandert (1) het politiewerk door de inzet van nieuwe technologie, ook heeft zij gevolgen voor (2) de politieorganisatie, (3) waar de politie zich op richt, en (4) waarmee zij wordt geconfronteerd.

Tegelijk is technologie niet iets wat de politieorganisatie ‘overkomt’: het zijn personen die technologie ontwikkelen, inzetten en erop reageren. Het is van belang – zeker met de verdere toepassing van data en AI in het politiewerk – dit perspectief vast te houden. Het betekent dat er keuzes zijn te maken, verantwoordelijkheid moet worden genomen, en verantwoording moet worden afgelegd.

Hoofdpijnen van het advies

Op het gebied van data en AI gebeurt binnen en buiten de politieorganisatie veel.¹⁰ Een volledig overzicht hiervan is lastig te geven, mede omdat de ontwikkelingen snel gaan en er weinig afstemming is tussen de talrijke initiatieven op verschillende plekken binnen de politie.¹¹ Hoewel de innovatiekracht binnen de organisatie waardevol is, brengt innovatie zonder regie, heldere kaders en passende regelgeving risico’s met zich mee. Het gaat dan om risico’s die mogelijk de democratische legitimiteit en de rechtstatelijke verankering van het politiewerk ondermijnen waardoor politiemensen in een zogeheten ‘niemandsland’ belanden – zonder duidelijke richtlijnen of bescherming. Anders gezegd, het gebruik van data en AI in het politiewerk moet bijdragen aan publieke waarden als veiligheid en efficiency, maar dit dient ook democratisch geborgd en rechtstatelijk te worden verankerd.

Wat zijn de belangrijkste uitdagingen ten aanzien van het navigeren in dit niemandsland? Een eerste constatering is het belang van een adequaat *wettelijk kader* en het daarmee verbonden toezicht.¹² Dit thema is niet nieuw. In 2018 zijn de hieronder aangehaalde knelpunten al door de commissie Koops beschreven.¹³ Opvallend is dat er sindsdien nauwelijks concrete opvolging heeft plaatsgevonden, terwijl de problematiek in de praktijk alleen maar urgenter wordt. Het doel van het eerste advies is daarom om deze problematiek opnieuw onder de aandacht te brengen.¹⁴ Daarnaast identificeert de Raad – op basis van de literatuur en input van experts – zes andere urgente uitdagingen op het gebied van data en AI die zowel de kwaliteit als de legitimiteit (formeel en sociaal) raken van politieoptreden – en in bredere zin van ‘de politie’.

Uitdaging 1: Een adequaat wettelijk kader

De mogelijkheden van big data en AI voor de uitvoering van de politietaak worden steeds groter. Dit leidt er onder andere toe dat de politie steeds meer data verzamelt en verwerkt van personen tegen wie geen verdenking van een strafbaar feit bestaat. Om in deze ontwikkelingen de grondrechten van burgers beter te beschermen wordt zowel op nationaal als Europees niveau gewerkt aan nieuwe wetgeving en richtlijnen. Op Europees niveau is een groot aantal juridische kaders op het gebied van data en algoritmen opgesteld, waarbij in de context van AI en politiewerk onder meer moet worden gedacht aan de *Law Enforcement Directive* (LED) en de *Artificial Intelligence Act* (AI Act). Op nationaal niveau is er gewerkt aan de modernisering van het Wetboek van Strafvordering (WvSv), met daarin meer aandacht voor het reguleren van nieuwe opsporingsbevoegdheden in een digitale omgeving.

Met betrekking tot nationale wetgeving valt het volgende op. De *vergaring* van gegevens door de politie wordt genormeerd in het WvSv. Maar de ontwikkelingen rondom datagedreven werken zijn ook onlosmakelijk verbonden aan de Wet Politiegegevens (Wpg). Hierin is het *verwerken* van gegevens door de politie geregeld. Tussen de normering van het vergaren en het verwerken van gegevens bestaat in het huidige wettelijke kader een harde knip. Bij datagedreven werken is er echter een voortdurende wisselwerking tussen de vergaring van gegevens en de verwerking hiervan. Een goed wettelijk kader voor datagedreven werken is daarom gebouwd op de visie dat vergaren en verwerken van gegevens niet los van elkaar kunnen worden gezien. Het ontbreken van een dergelijk kader belemmert een verdere legitieme en professionele ontwikkeling van de politie rondom datagedreven (samen)werken.

De Raad constateert dat herziening van de huidige wetgeving ten aanzien van de vergaring en de verwerking van gegevens noodzakelijk en urgent is. Het ontbreken van een adequaat wettelijk kader voor datagedreven werken leidt ertoe dat de grondrechten van burgers onvoldoende worden beschermd¹⁵ en dat de operationele strategie van de politie – als het gaat om datagedreven werken – hierdoor onder druk komt te staan.

Overheidsorganisaties die grote hoeveelheden gevoelige gegevens van burgers verwerken, kunnen daarnaast niet zonder professioneel en onafhankelijk toezicht dat de volle breedte bestrijkt van de activiteiten die hiervoor nodig zijn: vooraf, tijdens en achteraf. De Raad hecht aan zulk ‘end-to-end’ toezicht; niet uit wantrouwen tegenover de politie, maar ter bevordering van professionaliteit en maatschappelijk vertrouwen. In gevoerde achtergrondgesprekken met politieprofessionals in het digitale domein ziet de Raad een openheid voor – en ook behoefte aan – zulk onafhankelijk toezicht.

De Raad adviseert dat een evaluatiecommissie Wet politiegegevens wordt ingesteld vergelijkbaar met de evaluatiecommissie Wet op de inlichtingen- en veiligheidsdiensten. Voor deze nieuw in te stellen commissie zijn twee onderwerpen van belang:

- Wisselwerking van vergaren en verwerken van gegevens;
- Professioneel en onafhankelijk toezicht.

Uitdaging 2: Een overkoepelend ELSA (Ethical, Legal and Societal Aspects) raamwerk

ELSA gaat over maatschappelijk verantwoorde innovatie, waarbij rekening wordt gehouden met ethische, juridische en maatschappelijke aspecten bij het ontwerp en de inzet van nieuwe technologie. Belangrijk hierbij is om in een zo vroeg mogelijk stadium relevante stakeholders –bedrijven, burgers, maatschappelijke organisaties, wetenschap – te betrekken en te verbinden. Het onderliggende idee is dat op deze manier uiteenlopende waarden vanuit een breed perspectief in kaart worden gebracht en democratische afwegingen kunnen worden gemaakt daar waar ethische en juridische dilemma's optreden. Dit stimuleert een maatschappelijk verantwoord innovatieproces.¹⁶

Toepassingen op het werkterrein van de politie hebben vergaande gevolgen en zijn daarmee – terecht – vaak onderwerp van aandacht in de media en politiek. Daarbij gaat het onder meer over de ongewenste – feitelijke of mogelijke – uitkomsten van risicotaxatie-instrumenten en AI-toepassingen om criminaliteit op te sporen of te voorkomen. De politie is zich daarvan bewust en dat vertaalt zich ook in beleid, onder meer door versterking van compliance bij datagedreven werken in de strategische agenda¹⁷ en het opstellen van een Kwaliteitskader Big Data.¹⁸ Waar het gaat om (risicovolle) algoritmen en AI liggen hier ook verplichtingen die voortkomen uit Europese wet- en regelgeving, onder andere de ontwikkeling van een kwaliteits- en risicomanagementsysteem voor algoritmen en AI.¹⁹

Het betrekken van alle in de ELSA-methodiek genoemde stakeholders – waaronder burgers – is niet eenvoudig.²⁰ De politie experimenteert hiermee door zogenoemde 'ethiektafels' te organiseren waarbij verschillende publieke waarden en effecten in kaart worden gebracht in concrete casussen.²¹ Dat is prijzenswaardig, maar dit alles staat nog ver af van een structurele en duurzame inrichting van maatschappelijk verantwoorde innovatie. Daartoe is een overkoepelend ELSA-raamwerk en bijbehorende standaard-werkwijze nodig. In dit verband kan ook naar het buitenland worden gekeken. Een actueel voorbeeld uit het Verenigd Koninkrijk is de in 2024 gepubliceerde *New Machine Learning Guide for Policing*.²²

Publieke transparantie is een noodzakelijke voorwaarde voor de invulling van de maatschappelijke dimensie van ELSA. Dat geldt des te meer bij de ontwikkeling en inzet van (risicovolle) algoritmen en AI. De Raad benadrukt hierbij het belang van ‘actieve transparantie’, dat wil zeggen: ‘openbaar, tenzij’.²³ Actieve transparantie is verbonden met de opvolger van de Wet openbaarheid van bestuur (Wob) die de toegang tot overheidsinformatie regelt, de Wet open overheid (Woo). Het doel van de wet is een overheid die transparant is over haar functioneren en die zorgt dat informatie toegankelijk is voor iedereen. De wet regelt dat in beginsel alle overheidsinformatie openbaar is. Alleen bij uitzondering wordt hiervan afgeweken.²⁴ Ook in de Strategische agenda politie 2025-2030, *Stevig staan in deze tijd*, wordt onder de noemer van het versterken van rechtsstatelijk handelen het belang van meer maatschappelijke transparantie benadrukt. Dat gaat verder dan voldoen aan de wettelijke verplichtingen. Voor behoud van het vertrouwen in de politie is actieve transparantie – in het bijzonder waar het data- en AI-toepassingen betreft – cruciaal. Actieve transparantie betekent ook actief communiceren waar van de openbaarheid wordt afgeweken – en waarom.

De Raad adviseert om ELSA-afwegingen – en de daaruit voortvloeiende inzichten – structureel te integreren in het ontwikkelproces van data- en AI-toepassingen binnen de politie. Daarvoor is een overkoepelend ELSA-raamwerk nodig dat als standaard dient bij het ontwikkelen, aanschaffen en gebruiken van nieuwe toepassingen op het gebied van data en AI. Actieve transparantie moet daarbij de regel zijn: openbaar, tenzij. Als openbaarheid wordt beperkt, dient hierover op een overtuigende en navolgbare manier verantwoording te worden afgelegd.

Uitdaging 3: Formuleren van voorwaarden voor de samenwerking met private partijen

Voor datagedreven werken en de inzet van AI is samenwerking met private partijen onvermijdelijk.²⁵ Meer nog dan bij het klassieke fysiek waken over de veiligheid in de publieke ruimte is de politie als het gaat om digitalisering in bepaalde mate afhankelijk van het bedrijfsleven. Veel van de nieuwste AI-technologie is in handen van private partijen die hun producten en diensten graag verkopen aan of delen met de politie. De politie beschikt niet altijd over de benodigde kennis en expertise om dergelijke technologie zelf te ontwikkelen of te beheren, en is daardoor in zekere mate afhankelijk van commerciële partijen. Deze afhankelijkheid kent een aantal risico's voor de politie.

Systematische uitbesteding van opgaven op datagedreven werken of AI aan private partijen kan leiden tot 'weglekken' van essentiële kennis en kunde binnen de organisatie, die nodig zijn om sturing te geven en te kunnen monitoren.²⁶ Enkel zicht hebben op de procesmatige kant ervan is geen garantie voor een goede uitvoering. Dit vraagt ook om inhoudelijke *know-how*. In het verlengde hiervan is er het risico op *vendor lock-in*, waarbij de politie met handen en voeten is gebonden omdat bepaalde taken en vaardigheden waarvoor zij onvoldoende kennis heeft, zijn uitbesteed aan commerciële partijen. In beide gevallen is het belangrijk dat de politie voorafgaand aan een samenwerkingsverband nadenkt over hoe zij hierbinnen werkt aan haar eigen kennispositie en de borging hiervan binnen de politieorganisatie. Als het gaat om de inkoop van AI-toepassingen bij private partijen is een goede kennisbasis binnen de politie noodzakelijk om vooraf zelf te kunnen toetsen waar het betreffende algoritme op is getraind, of er sprake is van schone datasets, en hoe het algoritme werkt met politiedata. De Europese AI Act stelt dat ook bij inkoop van AI-tools de gebruiker van het algoritme verantwoordelijk is voor de inzet hiervan.

De afhankelijkheid van private partijen kan de opsporing van criminaliteit direct raken. Private partijen – al dan niet actief in de veiligheidszorg – beschikken vaak over *non-police datasets* die groter en gevarieerder zijn dan de datasets van de politie. Deze datasets kunnen voor de opsporing van bepaalde vormen van criminaliteit waardevol zijn als het gaat om zicht krijgen op nieuwe criminaliteitsfenomenen en op mogelijke verdachten die tot

dan toe onder de radar zijn gebleven. Voor de politie zit er een spanning op hoe zij gebruik kan maken van deze datasets. Het ontbreekt aan een juridische grondslag om deze datasets volledig binnen te halen en hier zelf analyses op te kunnen doen, omdat er vaak geen sprake van doelbinding zal zijn conform de Algemene verordening gegevensbescherming (AVG). Het delen van data met private partijen zodat zij de analyses kunnen uitvoeren, is echter uitgesloten vanwege het grote afbreukrisico.

Een vraag die door de huidige geopolitieke ontwikkelingen voor de politie nadrukkelijker op de voorgrond komt te staan, is hoe om te gaan met de afhankelijkheid van private partijen, met name de grote technologie-bedrijven.²⁷ Volledige digitale soevereiniteit is voor de politie niet haalbaar.²⁸ Desondanks hecht de Raad eraan om het belang van dit vraagstuk te benadrukken, onder meer vanwege de gevoeligheid van politiegegevens en het geweldsmonopolie van de politie. Bouwen aan digitale soevereiniteit kan betekenen dat er onder voorwaarden samengewerkt wordt met private partijen, mits er vooraf helderheid is over de eventuele risico's hiervan. Op grond van deze risicoanalyse kan telkens een afgewogen besluit worden genomen over hoe wordt samengewerkt. Daarbij moet in de risicoanalyse ook rekening worden gehouden met geopolitieke ontwikkelingen en mogelijke afhankelijkheid van staten met andere rechtsstelsels of belangen.

De Raad adviseert een toetsings- en samenwerkingskader op te stellen met duidelijke voorwaarden voor samenwerking met private partijen. De voorwaarden faciliteren dat de politie in publiek-private samenwerkingen zorgvuldig, verantwoord en doelgericht kan opereren. Het vastleggen van voorwaarden hiervoor draagt ook bij aan meer transparantie naar burgers en andere publieke en private partijen. Dat versterkt het maatschappelijk vertrouwen dat de politie in haar omgang met data en AI-toepassingen rechtsstatelijk en verantwoord handelt.

Uitdaging 4: Governance strategie datahuishouding

Datagedreven werken en de inzet van AI-toepassingen zijn niet alleen technologische, maar ook organisatorische vraagstukken. Anders gezegd, het is een sociaal-technologische opgave voor de politie. Een belangrijk onderwerp hierbij is het goed inrichten van een datahuishouding met voldoende *checks and balances*. Publieke waarden die hierbij een rol spelen zijn onder meer transparantie en *accountability*. Het omgaan met data – van de borging van kwaliteit ('vuile data') en het delen van informatie tot het in acht nemen van verwerkings- en bewaartermijnen (*privacy compliance*) – blijkt echter geen eenvoudige opgave voor de politie.²⁹ In de Strategische agenda politie 2025-2030 wordt het als volgt geformuleerd: 'Op dit moment zijn wij onvoldoende in staat om de hygiëne en integriteit van de data te (waar) borgen en te garanderen. Data worden bijvoorbeeld niet altijd op de juiste grondslagen verwerkt, wij zijn niet altijd in staat om voldoende zichtbaar te maken waar data vandaan komen en data worden soms niet op tijd verwijderd'.³⁰

De politie is geen eenvoudig te besturen institutie. De feitelijke organisatie kent drie niveaus: landelijk, regionaal, lokaal. Daarnaast zijn er binnen deze niveaus verschillende portefeuilles, waaronder de generieke opsporing, specialistische opsporing, *intelligence*, en gebiedsgebonden politiewerk die ook op alle drie de niveaus georganiseerd zijn. Data en AI raken steeds meer met elkaar verbonden en zijn van overstijgend belang voor de verschillende niveaus en portefeuille-onderwerpen. Voor innovatie en datagedreven werken heeft de politie een aparte governance structuur waar ook besluitvorming plaatsvindt. Daarbij zijn veel afhankelijkheden die invloed hebben op de allocatie van budgetten. Om besluitvorming goed te laten verlopen, is kennis van data en AI nodig binnen alle lagen van de organisatie – van operationeel tot tactisch en strategisch niveau. De Raad ziet daarbij een spanningsveld tussen de ontwikkeling van governance op deelterreinen in relatie tot data en AI en de governance van de organisatie als geheel.

Gelet op de ontwikkeling dat datagedreven werk in toenemende mate centraal komt te staan binnen de politie, zijn meer sturing en regie nodig op de datahuishouding (en daarmee: de datakwaliteit) van de politieorganisatie. Daarbij gaat het onder meer om het beter borgen van data- en AI-procesen in de politieorganisatie en het afleggen van verantwoording over het

gebruik ervan. De Raad meent bovendien dat er een goed overzicht nodig is van wat er binnen de politie al beschikbaar is, waaronder risicotaxatie-instrumenten en AI-toepassingen, ook om het risico van *shadow-AI* – informeel gebruik van AI-toepassingen door medewerkers – te verkleinen.³¹ De datacatalogus is een ontwikkeling die hierop aansluit; een (openbaar) algoritmeregister zou volgens de Raad een passende toevoeging zijn.

Met betrekking tot toekomstbestendige strategie op governance rondom data en AI **adviseert de Raad** besluitvorming over data en AI-toepassingen meer te verankeren in de bredere governance van de organisatie. Hierbij is duidelijkheid nodig over welke typen besluiten waar in de organisatie genomen worden. Daarnaast zijn meer regie en sturing op bestaande en lopende ontwikkelingen rondom de datahuis-houding noodzakelijk om interne en externe transparantie en accountability te bewerkstelligen.

Uitdaging 5: Data- en AI-geletterdheid als integrale basisvaardigheid

Data- en AI-toepassingen zijn er ter ondersteuning van politieprofessionals bij het uitvoeren van de taakopdracht (art. 3 Politiewet). Net als fysieke geweldsmiddelen, waaronder het dienstpistool en wapenstok, vergen zij kennis en training, maar zij onderscheiden zich door hun vaak onzichtbare, veranderlijke en complexe karakter. Daarom moet het begrijpen en verantwoord kunnen toepassen van data- en AI-systemen een basisvaardigheid worden binnen de politieorganisatie. Dit vraagt om structurele inbedding in het basis-, vakspecialistisch en hoger politieonderwijs – en in andere leertrajecten binnen de politieorganisatie.

Dit thema staat onder de noemer ‘digitale vaardigheid’ op de politie-agenda. De Politieonderwijsraad (POR) bracht hierover in 2020 het advies *Let’s get digital* uit.³² Binnen de politie wordt volop gewerkt aan digitale vaardigheid³³ en er zijn tal van initiatieven om de benodigde kennis beschikbaar te maken voor de basispolitiezorg.³⁴ Recente aandacht gaat specifiek uit naar data- en AI-geletterdheid. Daarbij is een centrale vraag hoe deze begrippen precies gedefinieerd kunnen worden, welke leerdoelen daaraan verbonden zijn, en hoe het onderwijs hierin actueel en toetsbaar kan blijven.

Naast formeel onderwijs zijn diverse leervormen van belang. Een veelbelovende aanpak is differentiëren op functieniveau, bijvoorbeeld via het model van datavolwassenheid en zogeheten *learning communities*.³⁵ Daarin leren medewerkers op hun eigen niveau, vanuit praktijkproblemen, mét en van elkaar. Ook microtrainingen kunnen hieraan bijdragen. Essentieel is dat wordt vastgesteld wie op welk niveau welke mate van data- en AI-geletterdheid nodig heeft.

De Raad waarschuwt voor het ontstaan van een ongewenste tweedeling binnen de politie tussen professionals die wel digitaal bekwaam zijn (‘experts’) en collega’s die dat niet zijn. Dit kan het vertalen en doorgeven van kennis en informatie door de organisatie heen en het bewustzijn van de risico’s van werken met data en AI-toepassingen belemmeren. Om dit scenario te voorkomen, zijn er verschillende initiatieven binnen de politie die zich richten op het algemeen versterken van data- en AI-geletterdheid ‘on the job’ en zijn

verschillende netwerken in het leven geroepen om de kennis en expertise te delen.³⁶

Volgens de Raad is het van belang dat medewerkers door de hele organisatie heen – naast het leren van praktische digitale vaardigheden – een kritische digitale *mindset* ontwikkelen in het omgaan met data en AI. Dat betekent: in staat zijn om vraagstukken systematisch te benaderen, bewust na te denken over de probleemdefinitie, datakeuze, verwerking, en de maatschappelijke implicaties van het gebruik. Hierbij worden de gestelde kaders gezien als onderdeel van het werk in plaats van als beperking. Dat dient ook zwaar te wegen bij de werving en selectie van nieuw personeel.

Het ontwikkelen van een kritische digitale *mindset* sluit aan bij de bredere opgave van de politie om rechtsstatelijk handelen in het digitale domein te waarborgen.³⁷ Waar in het fysieke optreden politiemensen doordrongen zijn van de rechtsstatelijke vereisten – zoals legaliteit, proportionaliteit en subsidiariteit – geldt die vanzelfsprekendheid niet voor data- en AI-toepassingen. Juist daarom is het belangrijk dat de organisatie voortdurend zicht houdt op hoe medewerkers omgaan met data en technologie: beschikken zij – in relatie tot hun functie – over voldoende kennis, vaardigheden en digitale oordeelskracht om verantwoord te handelen?

De Raad adviseert data- en AI-geletterdheid vorm te geven als een integrale basisvaardigheid, zowel via reguliere opleidingen als via *learning communities*. Het leren van en met elkaar en het direct kunnen toepassen van opgedane kennis (bijvoorbeeld via microtrainingen) is daarvoor cruciaal. De ontwikkeling van een kritische digitale *mindset* – in relatie tot het eigen werk – dient centraal te staan om blijvend de juiste afwegingen te maken bij het realiseren van uiteenlopende (en vaak conflicterende) publieke waarden. De Raad adviseert ten aanzien van de kritische digitale *mindset* om vast te stellen hoe het daar nu mee staat en de ontwikkeling daarvan door de tijd te blijven monitoren.

Uitdaging 6: Bredere kijk op toepassingsgebieden

De nadruk op het gebied van AI lijkt nu vooral te liggen op de strafrechtelijke rechtshandhaving, in het bijzonder waar het gaat om de bestrijding van georganiseerde criminaliteit. Het succesvol verwerven van afgeschermd data – met als bekende voorbeelden Ennetcom en Encrochat – en de analyse daarvan hebben de aard van opsporing ingrijpend veranderd. Daarnaast worden er veel praktische toepassingen ontwikkeld waarbij vaak operationele vragen vanuit de praktijk het vertrekpunt vormen.³⁸ Daarbij ligt de nadruk – naast het automatiseren van routinematige handelingen – op een efficiëntere en effectieve toegang tot (informatie uit) data.

De Raad constateert dat er minder aandacht is voor de vraag hoe AI kan bijdragen aan andere toepassingsgebieden, zoals de versterking van de relatie tussen politie en burgers en het daarop gebaseerde vertrouwen. Kunnen AI-toepassingen worden ingezet door de politie om haar sociale legitimiteit te versterken en te zorgen dat de relatie met burgers minder afstandelijk en onpersoonlijk ('abstract') wordt? Het gaat hierbij om andere typen toepassingen als de inmiddels 'bekende' voorbeelden van chatbots en virtuele agenten. Het gaat over vragen als op welke wijze AI-toepassingen kunnen helpen bij het inhoud geven aan uitgangspunten van *community policing* zoals probleemgericht werken en burgerbetrokkenheid, bijvoorbeeld door de inzet van technologie bij het gezamenlijk met de gemeenschap in kaart brengen van (on)veiligheid en mogelijke interventies.³⁹ Inspiratie hiervoor zou opgedaan kunnen worden bij het Europese project KOBAN, waarbij in verschillende politiepijots wordt geëxperimenteerd met datagedreven tools om lokale verbindingen tussen burgers en politie te versterken.⁴⁰

Daarnaast kan worden gekeken naar ontwikkelingen in andere domeinen, waaronder de gezondheidszorg. Pijots met Gen-AI in de eerstelijnszorg laten zien dat automatisering van gespreksverslagen niet alleen leidt tot meer efficiëntie van werkprocessen, maar ook tot minder mentale belasting van de professionals en een betere ervaren band met de patiënt.⁴¹ Dit sluit aan bij een recente ontwikkeling binnen de politie om een interne AI-toepassing 'spraak naar tekst' breed in te zetten tijdens bijvoorbeeld verhoren, meldkamer meldingen, en observaties op een plaats delict. Daarnaast wordt er geëxperimenteerd met de Intelligente Geografische Meldkamer Assistent, die de centralist gaat ondersteunen om mogelijke vluchtroutes van

verdachten te berekenen en inzetvoorstellen te doen voor beschikbare eenheden. Deze toepassingen bieden – naast operationele voordelen – mogelijk ook kansen in het versterken van de relatie met burgers.

De Raad adviseert meer te kijken naar data en AI-toepassingen die mogelijkheden bieden waar het gaat om het versterken van de relatie met en het vertrouwen van burgers ('positieve veiligheid'). Dit verandert in positieve zin mogelijk ook het maatschappelijke debat over de inzet van data- en AI-toepassingen door de politie.

Uitdaging 7: De effectiviteit van (voorspellende) datatoepassingen

Nieuwe technologische ontwikkelingen spreken tot de verbeelding en de toepassing daarvan wordt ook vaak gepresenteerd als onontkoombaar (*AI-common sense*). Bij de overheid – en meer specifiek bij de politie – gaat het bij de beoordeling van ‘nut en noodzaak’ van nieuwe toepassingen idealiter altijd om de drieslag doelmatigheid (efficiëntie), doeltreffendheid (effectiviteit) en legitimiteit. Bij de ontwikkeling en inzet van data- en AI-toepassingen is het zicht op effectiviteit vaak nog beperkt.⁴² Het ontbreekt in veel gevallen aan stevige evaluaties, terwijl zonder inzicht in de effectiviteit het ook problematisch is om publieke waarden als proportionaliteit en subsidiariteit – en daarmee legitimiteit – inhoud te geven.

De Raad pleit voor meer empirisch – zowel kwantitatief als kwalitatief – onderzoek naar de effectiviteit van door de politie ingezette technologieën op het gebied van data en AI. Daarbij gaat het niet alleen om 1) de instrumentele vraag of er een effect is op bijvoorbeeld de criminaliteit, maar ook 2) over de vraag ‘waarom en onder welke omstandigheden’ een toepassing wel of niet werkt, en of 3) inzetten wel wenselijk en uitlegbaar is (‘normatieve context’).

Een specifieke categorie van data- en AI-toepassingen binnen de politie richt zich op voorspellen. Door toegenomen technologische mogelijkheden is vooral criminaliteitsvoorspelling (*predictive policing*, *crime forecasting*) een snelgroeiend veld. De evaluaties die er zijn, op het gebied van *predictive policing* bijvoorbeeld, laten vooralsnog wisselende resultaten zien.⁴³ Data-toepassingen om geografisch te voorspellen hebben nu nog de overhand, maar net als in andere domeinen – het weer, virusuitbraken – blijkt accuraatheid op het lokale niveau een uitdaging. Een belangrijke reden daarvoor is de sterke contextafhankelijkheid, en in het criminaliteitsdomein in het bijzonder de afhankelijkheid van menselijk gedrag.

De vraag is of de politie wel sterk moet inzetten op ‘vooruitkijken’ en of de effectiviteit van ‘real time intelligence’ en ‘terugkijken’ niet veel groter is. De Raad realiseert zich dat een strikt onderscheid tussen deze drie catego-

rieën soms lastig is te maken. Maar de grote successen die de politie tot nu toe heeft geboekt, gaan vooral om toepassingen die – strikt gezien – niet ‘vooruitkijken’. Ten opzichte van de begindagen van het ‘voorspellen’ (denk aan de landelijke invoering van het Criminaliteits Anticipatie Systeem⁴⁴) zijn ook de aard en omvang van criminaliteit ingrijpend veranderd. Tegelijk hebben zich grote veranderingen voorgedaan in de aard en beschikbaarheid van data en typen AI-toepassingen.

De afgelopen vijftien jaar hebben bovendien laten zien dat voorspellen op persoonsniveau hoge en ingrijpende risico’s met zich meebrengt.⁴⁵ De effectiviteit is dikwijls onduidelijk en het is onwenselijk vanuit het perspectief van het vertrouwen dat burgers al dan niet hebben in de politie. Menselijk gedrag is slecht voorspelbaar en het is ook niet duidelijk welke variabelen er in een specifieke sociale context ertoe doen, hoe deze zijn te meten en vast te leggen. Voorspellen – bijvoorbeeld door het toekennen van een risico-score – kan leiden tot onjuiste conclusies met grote consequenties. Bovendien beschikken sommige groepen burgers – vaak in kwetsbare posities – over meer digitale ‘sporen’ dan anderen, wat kan leiden tot onevenredige aandacht. Het feit dat daders achteraf soms gemeenschappelijke kenmerken hebben, rechtvaardigt nog niet het voorspellen van gedrag. Voorspellen op persoonsniveau vergroot het risico op ongelijke behandeling, ondermijnt het vertrouwen in de politie en is zowel wetenschappelijk als normatief problematisch.

De conclusie lijkt daarom gerechtvaardigd dat het ‘voorspellen’ van crimineel gedrag op persoonsniveau geen vanzelfsprekende ambitie zou moeten zijn. Dit in tegenstelling tot de verdere inzet van data- en AI-toepassingen bij het analyseren van criminaliteitsfenomenen en – patronen op basis van historische en in sommige gevallen mogelijk *real time* data.

De Raad adviseert de politie niet verder in te zetten op (algoritmische) toepassingen die gericht zijn op het voorspellen van (crimineel) gedrag op persoonsniveau en dat ook publiekelijk kenbaar te maken. Daarmee kunnen legitieme maatschappelijke zorgen worden weggenomen zonder dat dit ten koste gaat van de doelmatigheid en doeltreffendheid van het politieoptreden.

Tot slot

Bovenstaande zeven uitdagingen zijn bedoeld om ordening aan te brengen in de veelheid aan thema's ten aanzien van het werken met data en AI in het politiewerk. Uiteraard is er sprake van onderlinge verbondenheid tussen de verschillende uitdagingen. Ook zijn de adviezen verschillend van aard. Zo zijn de laatste twee uitdagingen meer inhoudelijk ingericht en een pleidooi voor steviger onderzoek hiernaar. Bij dit alles is de snelheid van ontwikkelingen hoog, wat leidt tot gevoelde urgentie en tegelijk tot het risico steeds achter de feiten aan te lopen. Hoe hiermee om te gaan, is onderdeel van de discussie die mede met dit advies wordt beoogd. Ten aanzien van de hier geformuleerde uitdagingen is de tijd van vrijblijvendheid en experimenteren voorbij.

Referenties

- Afzal, M. & P. Panagiotopoulos (2024). Data in Policing: An Integrative Review. *International Journal of Public Administration*, online first.
- Duggan, M.J. et al. (2025). Clinician Experiences with Ambient Scribe Technology to Assist with Documentation Burden and Efficiency. *JAMA Network Open*, 8(2), e2460637.
- Endedijk, M.D. & K. Cuyvers (2022). Self-regulation of professional learning: towards a new era of research. In: C. Harteis, D. Gijbels & E. Kyndt (eds.), *Research approaches on workplace learning: insights from a growing field* (pp. 219-237), Cham: Springer.
- Ericson, R. & K. Haggerty (1997). *Policing the Risk Society*. Toronto: University of Toronto Press.
- Ferguson, A.G. (2017). *The rise of big data policing. Surveillance, race, and the future of law enforcement*. New York University Press.
- Haque, R., Saxena, D., Weathington, K., Chudzik, J. & Guha, S. (2024). Are We Asking the Right Questions?: Designing for Community Stakeholders' Interactions with AI in Policing. In: *Proceedings of the CHI Conference on Human Factors in Computing Systems* (CHI '24), May 11--16, Honolulu.
- Henry, N. (2011). Federal contracting. Government's dependency on private contractors. In: D.C. Menzel & H.E. White (eds), *The State of Public Administration: Issues, Challenges and Opportunities* (pp. 221-237), London: Routledge.
- Landman, W. (2023). *Politiewerk aan de horizon. Technologie, criminaliteit en de toekomst van politiewerk*. Den Haag: Sdu Uitgevers.
- Lee, Y., B. Bradford & K. Posch (2024). The Effectiveness of Big Data-Driven Predictive Policing: Systematic Review. *Justice Evaluation Journal*, 7(2), 127-160.
- Leese, M. (2024). Staying in control of technology: predictive policing, democracy, and digital sovereignty. *Democratization*, 31, (5)5, 963-978.
- Mali, B., C. Bronkhorst-Giesen & M. den Hengst (2017). *Predictive policing: lessen voor de toekomst. Een evaluatie van de landelijke pilot*, Apeldoorn: Politie-academie.
- Mohler, G.O., M.B. Short, S. Malinowski & M. Johnson (2016). Randomized Controlled Field Trials of Predictive Policing, *Journal of the American Statistical Association*, 110(512), 399-1411.
- Moyakine, E. (2014). *The privatized art of war: private military and security companies and state responsibility for their unlawful conduct in conflict areas*. School of Human Rights Research Series, 67, Intersentia.

- Muir, R. & F. O'Connell (2025). *Policing and Artificial Intelligence*. Police Foundation.
<https://www.police-foundation.org.uk/publication/policing-and-artificial-intelligence/>
- Ratcliffe, J.H., R.B. Taylor, A.P. Askey, K. Thomas, J. Grasso, K. Bethel, R. Fisher & J. Koehnlein (2021). The Philadelphia predictive policing experiment. *Journal of Experimental Criminology*, 17(1), 15-41.
- Schuilenburg, M. (2024). *Making Surveillance Public. Why You Should Be More Woke about AI and Algorithms*. The Hague: Eleven International Publishing.
- Schuilenburg, M. & M. Soudijn (2023). AI-criminaliteit: Een verkenning van actuele verschijningsvormen. *Justitiële verkenningen*, (50)1, 12-29.
- Storbeck, M., G. Jacobs, M. Schuilenburg & R. van den Akker (2025). Surveillance experiences of extinction rebellion activists and police: Unpacking the technologization of Dutch protest policing. *Big Data & Society*, 12(1), online first.
- van Dijk, A., P. de Baets, L. Gunther Moor, E. Devroe & S. Zouridis (eds.) (2022). *Politie en rechtsstaat in de gedigitaliseerde samenleving*. Cahier Politiestudies, 62(1).
- Welten, B.J.A.M., A.J. van Dijk, A.M. de Bruin, F.C. Hoogewoning, G.F.S.J. Kuijlaars, L.O. Luinenburg, D. Roest & R.R.H. van Zeijst (2019). *Politiefunctie en rechtsstaat in de gedigitaliseerde samenleving. Positionering in een meervoudige context*. Gevraagd advies aan de korpschef, Nederlandse Politie.
- Willems, D. & R. Doeleman (2014). Predictive policing – wens of werkelijkheid? *Het Tijdschrift voor de Politie*, 76 (4/5), 39-42.
- WRR (2021). *Opgave AI. De nieuwe systeemtechnologie*. WRR-rapport 105.

Eindnoten

- 1 Zie o.a. Ferguson, 2017; Welten et al., 2019; van Dijk et al., 2022; Landman, 2023; Schuilenburg, 2024.
- 2 Ericson & Haggerty, 1997.
- 3 Afzal & Panagiotopoulos, 2024.
- 4 In de *Strategische agenda 2025-2030* (2025) is digitale transformatie een zogenoemd 'doorsnijdend' thema.
- 5 WRR, 2021: 12.
- 6 Het politieteam *Science & Technology* genereerde met ChatGPT op 22 mei 2023 een fascinerende Techscan in a day van 251 pagina's over voor de politie relevante technologische ontwikkelingen.
- 7 Zie bijvoorbeeld Politie (2023) *Intelligent verbonden in tijden van onzekerheid. Transformatie naar de Nederlandse politie van 2028*.
- 8 Schuilenburg & Soudijn, 2023.
- 9 De inzet van technologie heeft naast praktische ook meer principiële gevolgen. Bij wijze van voorbeeld (Nieuwsbrief AI-organisatie nr. 2- februari 2025): in het NWO-consortium AI-MAPS is onderzoek gedaan naar het 'chilling effect' bij de inzet van AI en slimme camera's bij de blokkadeactie van XR in den Haag op demonstranten en politieagenten. Het onderzoek biedt empirische inzichten hoe het toenemende gebruik van technologie leidt tot verschillende 'chilling effecten', waaronder gevoelens van extreme openheid en extreme voorzichtigheid (Storbeck et al., 2025).
- 10 De literatuur over AI en mogelijke toepassingen op het terrein van veiligheid is omvangrijk. Dat geldt ook voor de kritische beschouwingen over de negatieve gevolgen van de inzet van technologie. Dat geldt in mindere mate voor de vraagstukken rondom AI vanuit het perspectief van de politieorganisatie zelf. Een goed voorbeeld van een dergelijke beschouwing is de recente publicatie van de *Police Foundation: Policing and Artificial Intelligence* (Muir & O'Connell, 2025). Daarin worden de volgende uitdagingen geformuleerd: *culture, data-readiness, organisation, ethics, law, workforce, resources, abstract policing*.
- 11 Vanuit het programma Digitale transformatie is een landkaart gemaakt waarin verschillende, voornamelijk lokaal, ontwikkelde initiatieven inzichtelijk zijn gemaakt. Dit laat de reikwijdte en overlap goed zien.
- 12 Zie bijlage 1.
- 13 Commissie modernisering opsporingsonderzoek in het digitale tijdperk (Commissie Koops), rapport (2018). Regulering van opsporingsbevoegdheden in een digitale omgeving. <https://www.recht.nl/nieuws/strafrecht/167059/rapport-van-de-commissie-modernisering-opsporingsonderzoek>.
- 14 Een recent initiatief (2025) is de instelling van een commissie die zich buigt over de strafvorderlijke gegevensverwerking, waarbij de opdrachtoomschrijving aansluit bij het advies van de Raad. Met dit advies wil de Raad de urgentie van dit thema benadrukken.

- 15 De Autoriteit Persoonsgegevens (AP) heeft in maart 2025 een wetsvoorstel getoetst dat gaat over de vergaring en verwerking van gegevens door de politie en dat onderdeel is van de modernisering van het Wetboek van Strafvordering. De AP constateert dat dit voorstel burgers onvoldoende beschermt tegen mogelijke disproportionele schendingen van hun grondrechten. Zie: www.autoriteitpersoonsgegevens.nl/actueel/ap-nieuw-wetboek-van-strafvordering-bescherm-mensen-onvoldoende.
- 16 Zie: <https://www.kia-st.nl/kiast2024-2027/2-kader-omgeving-en-positionering/ethical-legal-and-societal-aspects-elsa-1>.
- 17 In de *Strategische agenda 2025-2030* wordt onder de noemer ‘rechtstatelijk handelen’ (2025: 19) ethiek en compliance bij datagedreven (samen)werken benoemd als focuspunt.
- 18 Zo is in 2020 binnen de opsporing het Kwaliteitskader Big Data opgesteld, dat op een methodologische wijze inzichtelijk moet maken hoe een big data-project wordt opgezet, uitgevoerd en of de *checks and balances* aanwezig zijn. Zie: <https://open.overheid.nl/documenten/ronl-ac9d5901-7d8d-44f7-ae89-3d305a2506d0/pdf>.
- 19 Zie: KRAAI (projectbeschrijving 2025). KRAAI is het nieuwe Kwaliteits- en Risicomanagementsysteem voor algoritmen en AI. Het helpt de politie om (risicovolle) algoritmen te beoordelen en te monitoren. De AI Act stelt duidelijke regels vast voor de inzet van AI-systemen. KRAAI ondersteunt de organisatie bij het voldoen aan die regels, onder meer door praktische hulpmiddelen en richtlijnen aan te bieden, waaronder:
 - Een multidisciplinaire adviescommissie die algoritmen beoordeelt en advies geeft;
 - Een algoritmebibliotheek voor overzicht en inzicht in alle algoritmen in ontwikkeling of gebruik;
 - Duidelijke richtlijnen voor ontwikkelen projectteams, zodat zij weten wat er van hen wordt verwacht.
- 20 Dit staat los van de veelheid aan contacten die er in algemene zin is met stakeholders waaronder mensenrechtenorganisaties en de wetenschap.
- 21 Zie onder meer de procesbeschrijving van de ethiektafels (2025) waarbij ook wordt ingegaan op wie er betrokken zijn. De stappen bij een ethiektafel zijn gebaseerd op de methodiek begeleidingsethiek van het ECP en zijn de volgende:
 1. Presentatie van de casus: Wat is de technologie en waarvoor wordt die gebruikt?
 2. Bespreking van risico's: Wat zijn de mogelijke gevolgen, bijvoorbeeld op het gebied van privacy of discriminatie?
 3. Oplossingen bedenken: Hoe kunnen risico's worden verkleind en kansen worden benut?
 4. Vastleggen van uitkomsten: De conclusies worden genoteerd in een ethisch logboek, zodat ze later kunnen worden herzien of aangepast.
- 22 Zie: <https://science.police.uk/news-and-events/news/new-machine-learning-guide-for-policing/>.
- 23 Dit is in lijn met de Strategische Agenda 2025-2030 waarin de politie onder de noemer rechtstatelijk handelen het belang van actiever inzicht geven in haar handelen benadrukt (2025: 19).
- 24 Zie: <https://www.informatiehuishouding.nl/leerhuis-en-campagnes/dewoodatzitso>.
- 25 Digitalisering roept ook vragen op over hoe hierin samen te werken met publieke partijen, bijvoorbeeld als het gaat om welke data onderling te delen en onder welke voorwaarden dit gebeurt. Binnen de politie is dit thema onderwerp van beleidsontwikkeling. Daarom wordt dit thema verder buiten beschouwing gelaten en richt de aandacht in dit advies zich op de samenwerking met private partijen.

- 26 Dit speelt ook in andere overheidsdomeinen. In het verleden werd dit bijvoorbeeld gezien bij de privatisering van defensietaken in de Verenigde Staten, zie o.a.: Henry, 2011; Moyakine, 2014.
- 27 Zie daarvoor bijvoorbeeld het Position paper van het Rathenau instituut voor het Rondetafelgesprek inzake digitale soevereiniteit bij de Rijksoverheid Tweede Kamer, Vaste commissie voor Digitale Zaken, 13 februari 2025. <https://www.rathenau.nl/nl/berichten-aan-het-parlement/rondetafelgesprek-digitale-soevereiniteit-bij-de-rijksoverheid>.
- 28 Leese, 2024.
- 29 Zie o.a. de conclusies van het rapport van de Raad van State (10 maart 2025) *Voorlichting over verlenging bewaartermijn politiegegevens*, waarbij wordt verwezen naar de volgende bronnen in relatie tot de datahuishouding van de politie: Kamerstukken II 2015-16, 33842, nr. 3 en bijlage (Auditdienst Rijk, Privacy audit Wpg 2015 Politie, 29 oktober 2015); Kamerstukken II 2019/20, 33842, nr. 5 en bijlage (Auditdienst Rijk, Assurancerapport Privacy audit Wpg 2019 Politie, 2 maart 2020); Kamerstukken II 2023/24, 29628, nr. 1190 en bijlage (KPMG, Nationale Politie: Privacy assurance-rapport inzake Wet politiegegevens (Wpg), 12 september 2023).
- 30 2025: 19.
- 31 Zie: <https://natlawreview.com/article/ai-governance-problem-shadow-ai>.
- 32 Zie ook de beleidsreactie van de Minister van V&J, 20 juni 2021 (3490731).
- 33 De opdracht van de korpsleiding Integrale digitale vaardigheid (2023) is erop gericht te zorgen dat alle politiemedewerkers digitaal vaardig worden en blijven, en hun kennis, vaardigheden en attitude aansluiten bij de gedigitaliseerde maatschappij. Dit door het realiseren van:
 - Digitaal bewustzijn, kennis en vaardigheden van de medewerkers;
 - Digitaal vaardige instroom van medewerkers (nieuw en bijscholing);
 - Digitaal leiderschap: coachend en begeleidend.
- 34 Menukaart Digitale Vaardigheid, GGP, mei 2024.
- 35 Endedijk & Cuyvers, 2022.
- 36 Een voorbeeld is het team VAK. Het doel van VAK is om de versnipperde domeinkennis op te halen en vast te leggen in crimescripts en (aanvullende) kennisdocumenten. VAK helpt invulling geven aan de kennis-randvoorwaarden voor effectief en efficiënt datagedreven werken (CSAE). Met andere woorden: het op orde hebben van domeinkennis (kennis over criminaliteit en middelen), datakennis (kennis over datavormen) en toolkennis (kennis over het gebruik van tools).
- 37 *Strategische Agenda 2025-2030* (2025: 18).
- 38 Een aansprekend voorbeeld is het Team Rendement Operationele Informatie (TROI) dat tal van tools ontwikkelt. Voor de politiemensen aan de basisteams (GGP en opsporing) zijn veel praktische tools beschikbaar en toegankelijk.
- 39 Haque et al., 2024.
- 40 Zie: <https://koban-project.eu/>.
- 41 Duggan et al., 2025.
- 42 Lee & Posch, 2024.
- 43 Zie o.a. Mohler et al., 2016; Mali, Bronkhorst-Giesen & Den Hengst, 2017; Ratcliffe et al., 2021.
- 44 Willems & Doeleman, 2014.

- 45 In dit verband zou ook moeten worden gekeken naar de negatieve gevolgen van risico-taxatie-instrumenten voor individuen en groepen personen (op basis van sociale klasse en etniciteit bijvoorbeeld). Zie hierover berichtgeving in de media over instrumenten als *Preselect Recidive* en *Geweld* (RTI-G): *Follow the Money* (20-01-2025) *Onbetrouwbaar algoritme bestempelt jongeren onterecht als toekomstig crimineel*; *Security.nl* (21-01-2025) *Justitie gebruikt algoritme om recidive risico jongeren te voorspellen*.

Bijlage I

Deeladvies Instellen evaluatiecommissie Wet politiegegevens

De wetenschappelijke adviesraad voor de Politie (WARP) adviseert de korpsleiding bij deze om samen met de minister van Justitie en Veiligheid te bewerkstelligen dat een Evaluatiecommissie Wet politiegegevens (Wpg) ingesteld wordt, met een opdracht en onafhankelijke statuut die vergelijkbaar is met de eerdere Evaluatiecommissie Wet op de inlichtingen- en veiligheidsdiensten 2017.¹

De WARP zelf heeft een te beperkte opdracht en capaciteit om een dergelijke evaluatie te verrichten. De problematiek die achter dit advies schuilgaat is daarbij complex. In onderstaande drie alinea's worden de achtergrond van het advies, alsmede twee relevante onderwerpen voor de voorgestelde evaluatie, geschetst.

Achtergrond: de datagedreven werkwijze die de laatste jaren brede opgang vindt binnen de politie

Binnen de opsporing worden grote hoeveelheden ('bulk') gegevens (her)verwerkt van personen tegen wie geen verdenking bestaat of zal ontstaan. Ook met het oog op voorkoming van openbare ordeverstoringen worden steeds vaker en meer data van burgers (her)verwerkt.² Het analyseren van grote gegevensbestanden kan nuttig zijn voor de verschillende taken van de

1 Voor meer informatie over deze evaluatiecommissie Wiv 2017, zie onder meer de [wettelijke regeling](#) of het [eindrapport](#).

2 Bijvoorbeeld door het Team Openbare Orde en Inlichtingen (TOOI), zie daarover – inclusief aandacht voor het wettelijk kader – M. den Hengst, T. ten Brink & J. ter Mors (2017). *Informatiegestuurd politiewerk in de praktijk*. Politieacademie/ Vakmedianet.

politie. Het is bovendien de nadrukkelijke ambitie van de politie om meer datagedreven te gaan werken.³

Een dergelijke werkwijze vereist een modern wettelijk kader waarin onderzoeksbelangen en bescherming van grondrechten zijn afgewogen tegen de achtergrond van technologische (on)mogelijkheden en op basis van een parlementair/publiek debat.⁴ De Wpg is in huidige vorm onvoldoende toegesneden op de beoogde datagedreven werkwijze.

Grondslagen voor grootschalige data-analyse: wisselwerking vergaren en verwerken

Een modern wettelijk kader voor datagedreven werken is gebouwd op de visie dat vergaren en verwerken van gegevens niet los van elkaar kunnen worden gezien. Zowel het vergaren, als het daaropvolgende (bewaren en) gebruiken maken inbreuk op privacy-rechten. De normering van de gebruiksmogelijkheden heeft invloed op de normering van de vergaringsmogelijkheden, en vice versa. Als immers het gebruik van gegevens na vergaring ruimer en indringender mogelijk is, wordt de normering van de vergaring zelf belangrijker. Als, omgekeerd, het gebruik van gegevens strikt is genormeerd, kan dat een ruimere vergaringsbevoegdheid rechtvaardigen.⁵ Ook uit Europese rechtspraak blijkt dat het gehele proces van vergaren en verwerken integraal moet worden benaderd, waarbij bovendien duidelijk is dat de grootste inbreuk op het recht op privacy ligt in het analysestuk en dan vooral in het combineren en hergebruiken van grote hoeveelheden gegevens.⁶

3 Landelijke Programmaplan, Magazine Datagedreven Samen Werken (2024).

4 Zie ook: B.W. Schermer, Het gebruik van Big Data voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens, *Tijdschrift voor Bijzonder Strafrecht en Handhaving* 2017/4; M.F.H. Hirsch Ballin & J.J. Oerlemans, Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden, *Delikt en Delinkwent* 2023/2; R.M. te Molder, M.J. Dubelaar, M.I. Fedorova, S.M.A. Lestrade & T.F. Walree, Naar een duidelijker juridisch kader voor geautomatiseerde data-analyse in de opsporing, *Computerrecht* 2023/64.

5 Commissie modernisering opsporingsonderzoek in het digitale tijdperk (Commissie Koops), Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 24-25.

6 Zie daarover uitgebreid (en met verwijzing naar andere auteurs en relevante rechtspraak): M.I. Fedorova, R.M. te Molder, M.J. Dubelaar, S.M.A. Lestrade, T.F. Walree (2022), *Strafvorderlijke gegevensverwerking. Een verkennende studie naar relevante gezichtspunten bij de normering van het verwerken van persoonsgegevens voor strafvorderlijke doeleinden*, Nijmegen: Radboud University Press.

Tussen de normering van het vergaren en het verwerken van gegevens bestaat in het huidige wettelijke kader echter een harde knip: het verwerken is geregeld in de Wpg, het vergaren in het Wetboek van Strafvordering en, bijvoorbeeld, in de Politiewet. Meerdere auteurs hebben erop gewezen dat de normeringskaders van de Wpg en Sv met elkaar verbonden moeten worden.⁷ Een kans daarvoor lag in de modernisering van het Wetboek van Strafvordering. In de voorstellen voor het gemoderniseerde Wetboek van Strafvordering wordt de knip echter – mede vanwege de complexiteit van het onderwerp – gehandhaafd.⁸ Dat betekent dat de *analyse* van grote hoeveelheden databestanden in de nabije toekomst niet in het Wetboek van Strafvordering zal worden genormeerd. Juist vanwege de grote ambities van de politie inzake datagedreven werken is die situatie risicovol. Een evaluatie van de Wpg maakt mogelijk dat die risico's worden onderzocht en dat, vanuit een integrale visie op vergaren en verwerken, voorstellen kunnen worden gedaan voor adequate wettelijke grondslagen voor datagedreven werken.

Het toezicht op de Wpg

Overheidsorganisaties die grote hoeveelheden gevoelige gegevens van burgers verwerken kunnen niet zonder professioneel en onafhankelijk toezicht dat de volle breedte van de activiteiten bestrijkt: vooraf, tijdens, en achteraf. De WARP hecht aan zulk 'end-to-end' toezicht, niet uit wantrouwen tegenover de politie, maar ter bevordering van professionaliteit en maatschappelijk vertrouwen. In enkele achtergrondgesprekken met politiemensen in het digitale domein ziet de WARP een openheid voor, en ook behoefte aan, zulk onafhankelijk toezicht. De digitale praktijk ontwikkelt zich snel en vereist regelmatig delicate afwegingen waarbij een institutioneel verankerde onafhankelijke toezichthouder met brede dekking de kwaliteit van de afwegingen en besluiten kan verhogen. Ook legt het Europese recht (zowel vanuit het EHRM als het HvJ EU) steeds meer de nadruk legt op de onafhankelijkheid van het toezicht.

7 Schermer 2017; Fedorova e.a. 2022; Hirsch Ballin & Oerlemans 2023.

8 Zie: Consultatieversie Memorie van toelichting eerste aanvullingswet nieuw Wetboek van Strafvordering, p. 18. Te raadplegen via [Overheid.nl](https://overheid.nl) | [Consultatie Eerste aanvullingswet nieuw Wetboek van Strafvordering \(internetconsultatie.nl\)](https://internetconsultatie.nl)

Als achtergrondinformatie volgt hieronder een korte schets van het huidige, versnipperde toezicht op (het functioneren van de Wpg bij) de politie. Deze schets is enkel bedoeld om een beeld te geven en heeft geen enkele pretentie om volledig te zijn.

- De (straf)rechter kan op zitting de rechtmatigheid van opsporingsbevoegdheden toetsen, inclusief het verwerven en verwerken van gegevens, maar hieraan zitten beperkingen. Dit is een toets ‘achteraf’. Niet al het onderzoek dat de politie verricht leidt tot een rechtszaak. Ook krijgen de digitale aspecten van het politieonderzoek in de rechtszaal niet altijd de aandacht die ze verdienen. Daar komt bij het belang van de niet-verdachte burger geen onderdeel uitmaakt van de rechtmatigheidstoets. Deze toets is gericht op het belang van de verdachte.
- De rechter-commissaris geeft al of niet een machtiging voor de inzet van bepaalde opsporingsbevoegdheden. Dit vormt een onafhankelijke toets, die in de praktijk beperkt is tot de fase ‘vooraf’. Digitaal onderzoek is dynamisch van aard en laat zich niet altijd goed ‘vooraf’, statisch toetsen.⁹
- De officier van justitie combineert twee rollen, die kortweg omschreven kunnen worden als crimefighter en magistraat. Het toezicht op de politie vanuit die magistratelijke rol past bij de fase ‘tijdens’. Het is zaaksgericht en geen breed, casusoverstijgend toezicht. In de praktijk is dit toezicht van de officier van justitie erop gericht om het requisitoir bij de rechter overeind te houden.
- De verwerking van persoonsgegevens voor doelen als het voorkomen, opsporen en onderzoeken van strafbare feiten door de politie valt onder de Richtlijn 2016/680 (ook wel aangeduid als: Law Enforcement Directive). Deze richtlijn is geïmplementeerd in de Wpg en wijst de Autoriteit Persoonsgegevens aan als toezichthouder. Deze autoriteit geeft invulling aan deze taak maar heeft tegelijkertijd te maken met een structureel capaciteitsprobleem.

9 De beperkingen van toezicht vooraf treden vooral op bij de hackbevoegdheid, zie: B. Jacobs, R. Jansen, ‘Hoe hackers vastlopen. Over uitvoeringsproblemen bij hackoperaties van de politie en van de inlichtingen- en veiligheidsdiensten’, *Computerrecht* 2024/3.

- De inspectie van het ministerie van Justitie en Veiligheid ziet toe op de uitvoering bij de politie – en daarnaast ook bij andere uitvoeringsdiensten binnen het ministerie, zoals het gevangeniswezen en de immigratiedienst. Deze inspectie van het eigen ministerie heeft vooralsnog geen bijzondere aandacht geschonken aan de Wpg in het algemeen en aan datagedreven werken in het bijzonder.
- Het interne toezicht van de politie zelf zou de hele uitvoeringspraktijk moeten beslaan maar functioneert suboptimaal. Het heeft vorig jaar een hard negatief oordeel ontvangen (drie rode blokken, in alle categorieën) in een onafhankelijk auditrapport.¹⁰

10 KPMG, Privacy assurance-rapport inzake Wet politiegegevens (Wpg), 12 september 2023. Dit rapport is op 20 oktober 2023 als bijlage van een [verzamelbrief](#) aan de Tweede Kamer gestuurd.

Colofon

Uitgave: Wetenschappelijke Adviesraad Politie (WARP)

Datum: Juni 2025

Redactie: Anne Tak

Vormgeving: Studio Tint, Den Haag

Drukwerk: Repro Amsterdam

Informatie: www.wetenschappelijkeadviesraadpolitie.nl

© Wetenschappelijke Adviesraad Politie (WARP), Den Haag 2025

