

AI-toepassingen in het politiewerk

Juridische vraagstukken in een datagedreven organisatie

Cahiers Politiestudies
Jaargang 2025-3, nr. 77
p. 313-326
© Gompel&Svacina
ISBN 978-94-6371-594-2



Marc Schuilenburg¹

Dit artikel beschrijft drie fasen van een AI-toepassing op basis van het theoretische concept van de 'AI-levenscyclus'. Ik laat zien hoe de verschillende fasen van een AI-toepassing voortdurend met elkaar verbonden zijn en daarom niet los van elkaar kunnen worden beschouwd. Ik concentreer me op de belangrijkste juridische kwesties op het gebied van wetshandhaving die zich in elk van deze drie fasen voordoen: input, throughput en output. In de conclusie vat ik de belangrijkste bevindingen samen en bespreek ik de verschillende aspecten van AI als sociaal-technologische uitdaging voor datagestuurd politiewerk.

1. Inleiding

De digitalisering en algoritmisering van het politiewerk is een socio-technologische opgave (o.a. Terpstra & Salet, 2020; Schuilenburg, 2024; Van Brakel & Govaerts, 2024; Hadjimatheou & Fussey, 2025). Dit betekent dat er een voortdurende interactie is tussen mens en techniek en dat daarmee klassieke opposities tussen het sociale en het technische ter discussie komen te staan (cf. Latour, 1993; 2005). Dit blijkt uit het gebruik van AI-toepassingen om de veiligheid te verbeteren. Het succes of falen hiervan ligt niet alleen in de technische kwaliteit van een AI-tool. Het ligt ook aan de wijze waarop een tool in de praktijk wordt gebruikt – en daarvoor is het afhankelijk van politieprofessionals van vlees en bloed. Zo verzamelt de politie grote hoeveelheden data (*big data*), die vervolgens met algoritmes worden geanalyseerd om op basis daarvan concrete acties te ondernemen, bijvoorbeeld de beslissing om meer agenten in te zetten op geïdentificeerde 'hot spots' – gebieden waarvan wordt verwacht dat er bepaalde vormen van criminaliteit (gaan) plaatsvinden (Schuilenburg, 2016; Hardyns & Rummens, 2017; Bennett Moses & Chan, 2018). Het inzetten van extra surveillance van agenten op deze plekken kan tal van ethische en juridische kwesties met zich meebrengen, waaronder discriminatie van minderheden, stigmatisering en *overpolicing* (o.a. Ferguson, 2017; Peeters & Schuilenburg, 2018; Benjamin, 2019; Van Brakel, 2023). Daarmee raken dergelijke AI-toepassingen de kern van de democratische

¹ Marc Schuilenburg is professor Digital Surveillance bij de Erasmus Universiteit Rotterdam.

rechtsstaat: het vertrouwen tussen burgers en overheid en de betrouwbaarheid van de overheid (Schuilenburg, 2025).

Over een betrouwbare overheid is in Nederland de afgelopen jaren veel te doen geweest. Zo werden in het Toeslagenschandaal risicoprofielen opgesteld op basis van het verboden onderscheid op grond van ras, waardoor aanvragers van kinderopvangtoeslagen met een tweede nationaliteit meer kans hadden gecontroleerd te worden door de Belastingdienst. Daarbij hadden de uitvoerende en rechtsprekende macht, zo oordeelde de Parlementaire enquêtecommissie Fraudebeleid en Dienstverlening in haar rapport *Blind voor mens en recht* (2024), veel te weinig oog voor de gevolgen van hun besluiten voor de aanvragers van de kinderopvangtoeslagen. Mede naar aanleiding van het Toeslagenschandaal wordt daarom ervoor gepleit om de verantwoordelijkheid voor een beslissing in AI-toepassingen neer te leggen bij personen van vlees en bloed. Dit is de kwestie van ‘human-in-the-loop’, waarbij professionals de kennis, kunde en middelen bezitten om een verkeerde beslissing te kunnen corrigeren.² Door ‘humans-in-the-loop’ te houden blijft menselijk maatwerk mogelijk en is er een aanwijsbaar persoon die verantwoordelijk kan worden gehouden voor concrete besluiten. In dat licht moet ook het streven van de Europese Unie worden begrepen om AI-toepassingen ‘mensgericht’ (*human-centric AI*) te maken.

De toegenomen aandacht en bewustzijn voor de menselijke factor bij het gebruik van AI-toepassingen heeft als keerzijde dat de technische kant uit het oog dreigt te worden verloren. Met de technische kant doel ik op (i) de kwaliteit van de data die worden gebruikt in de datasets van een AI-toepassing en (ii) de verwerking ervan via algoritmes om (iii) tot effectieve en efficiënte interventies te komen. Hoe nauwkeurig zijn de data bijvoorbeeld die de politie hiervoor gebruikt? Zijn alle data wel beschikbaar? Is er goed zicht op de werking van de algoritmes die de inputdata analyseren? Deze vragen zijn relevant omdat onvoldoende borging en zorg voor de kwaliteit van data kan leiden tot allerlei schendingen van fundamentele mensenrechten, van onvoldoende bescherming van de persoonlijke levenssfeer tot – hiervoor al kort benoemd – discriminatie van minderheden. Het is zelfs denkbaar dat de inzet van AI bij het verwerken van grote hoeveelheden data het recht op een eerlijk proces kan aantasten, zoals geformuleerd in artikel 6 van het Europees Verdrag voor de Rechten van de Mens (EVRM) (o.a. Commissie-Koops, 2018; Schermer & Oerlemans, 2020).

De inzet van AI-toepassingen in het politiewerk vraagt om voldoende juridische waarborgen voor de risico’s die hieraan kleven. De juridische problematiek op dit gebied is echter zo breed dat het noodzakelijk is om in te zoomen en daarbij een aantal keuzes te maken. Zo kunnen drie stadia van een AI-toepassing worden onderscheiden waarin relevante juridische vragen zich voordoen: de *input*, *throughput* en *output* (WRR, 2016; Peeters & Schuilenburg, 2023; Wessels, 2023; Schuilenburg, 2024). Daarbij richt ik mij in dit artikel op de juridische vragen op het gebied van de Nederlandse strafvordering. Het gaat hierbij onder meer om het regelen van onderzoeksbevoegdheden van de politie,

² In het veiligheidsdomein speelt deze thematiek op verschillende gebieden, waaronder de rechtspraak, waarbij rechters in grotere en complexere zaken worden vervangen door digitaal uitgespuwde computervonnissen (ook wel ‘robotrechtspraak’ genoemd). De discussie speelt ook bij de inzet van automatische en autonome systemen in oorlogsvoering, zoals onbemande vliegtuigstoelen, zwermen drones en *killer robots*. In de literatuur worden hierbij drie vormen van menselijke controle onderscheiden, namelijk waarbij de professional respectievelijk *in the loop*, *on the loop* en *out of the loop* is (Enarsson, Enqvist & Naarttijärvi, 2021).

waaronder het verzamelen en analyseren van data in AI-toepassingen. Dit betekent dat het zal gaan om AI-toepassingen die worden gebruikt in het kader van de opsporing en handhaving van strafbare delicten door de politie.

Hiertoe beschrijf ik eerst de drie stadia van een AI-toepassing en dit doe ik aan de hand van het theoretische concept van een AI-levenscyclus. Daarbij laat ik zien hoe de verschillende stadia van een AI-toepassing voortdurend in elkaar doorwerken en dus niet los van elkaar kunnen worden gezien. Vervolgens richt ik mij op de belangrijkste juridische vraagstukken op het gebied van de strafvordering die zich voordoen in ieder van deze drie stadia: de *input*, *throughput* en *output*. In de conclusie vat ik de belangrijkste resultaten samen en ga ik in op de verschillende kanten van AI als een socio-technologische opgave voor datagedreven politiewerk.

2. AI-levenscyclus en datagedreven politiewerk

AI is een verzamel- of overkoepelende term voor een grote groep van nieuwe technologieën die de laatste decennia in steeds meer domeinen worden gebruikt. In artikel 3 lid 1 van de AI-Act definieert de Europese Unie AI als volgt: “Een op een machine gebaseerd systeem dat is ontworpen om met verschillende niveaus van autonomie te werken en dat na het inzetten ervan aanpassingsvermogen kan vertonen, en dat, voor expliciete of impliciete doelstellingen, uit de ontvangen input afleidt hoe output te genereren zoals voorspellingen, inhoud, aanbevelingen of beslissingen die van invloed kunnen zijn op fysieke of virtuele omgevingen” (zie ook: High-Level Expert Group on Artificial Intelligence, 2019). Razendsnelle ontwikkelingen op het gebied van AI maken dat een uitputtende lijst van dergelijke systemen niet is te geven, maar in ieder geval kan hierbij worden gedacht aan toepassingen die nu al worden gebruikt binnen de opsporing en handhaving van criminaliteit, waaronder gezichts- en spraakherkenningssoftware, risico- en succesvoorspelling, algoritmische besluitvorming, realtime intelligence, online gegevensvergarig, cybercrime-opsporing, emotieherkenning, chatbots, enzovoort (Landman, 2023; Van Brakel, 2023; Schuilenburg, 2024). Deze AI-toepassingen worden door de politie ingezet op drie terreinen: werk op straat, opsporing en recherche, en intelligence (Schuilenburg & Soudijn, 2023; Afzal & Panagiotopoulos, 2024; Khalfa et al. 2024).

Elementair onderdeel van AI-toepassingen is de data waarmee wordt gewerkt en die Kitchin definieert als “bouwstenen waaruit informatie en kennis worden geproduceerd en die de input en output vormen van computationele processen” (2025: 45; zie ook: Bellanova, 2025). Met termen als ‘data flows’ (McNally et al. 2012), ‘data streams’ (Dourish & Gómez Cruz, 2018) en ‘data journeys’ (Leonelli, 2020) wordt gewezen op het feit dat digitale data op een andere manier circuleren als andere materialen in een organisatie. Kitchin et al. (2025) stellen dat in de circulatie van data er sprake is van een voortdurend proces van ‘replication, proliferation and data transformation’. Een goed voorbeeld hiervan is de toepassing ‘Raffinaderij’, een analyseomgeving van de Nederlandse politie waarin met specialistische AI-software van het Amerikaanse techbedrijf Palentir digitale politiegegevens en ruwe data over miljoenen Nederlanders met elkaar worden verbonden en doorzoekbaar worden gemaakt voor de opsporing van zware en georganiseerde criminaliteit en het voorkomen van aanslagen.³ Informatieproducten

³ Zie: Antwoorden Kamervragen over Palentir, 20 augustus 2025, <https://open.overheid.nl/documenten/848db95a-0456-4b12-93ab-1dd457d3a228/file>.

uit deze analyseomgeving worden gebruikt voor opsporingsonderzoek en kunnen aanleiding zijn voor het leggen van contact met andere partijen in de strafketen.

Het baseren van het politiewerk op geautomatiseerde analyses van grote hoeveelheden data past in een bredere ontwikkeling van de politie naar een datagedreven organisatie, wat, zo schrijft de politie in haar strategische agenda *Stevig staan in deze tijd*, “kan bijdragen aan beter politiewerk en het dienen van de waarden van de rechtsstaat” (2025: 19). Kern van datagedreven politiewerk is dat er sprake is van een cyclisch model dat uit verschillende fasen bestaat. Deze stadia bestaan uit het verzamelen, opslaan, analyseren en toepassen van data, waarbij de interventie – idealiter – steeds verder wordt geoptimaliseerd doordat op basis van de uitkomsten de interventie steeds opnieuw wordt aangepast.⁴ Hiervoor wordt de cybernetische term ‘feedback-processen’ gebruikt: systemen die reageren op hun eigen acties (Johnston, 2008). Zo meende de bekende cyberneticus Norbert Wiener dat het concept van feedback “zou kunnen helpen ‘intelligentie’ te verklaren” (Katz, 2020: 22) van zowel menselijke als niet-menselijke, natuurlijke en kunstmatige systemen. Letterlijk betekent feedback ‘terugvoeding’, ‘terugmelding’ of ‘terugkoppeling’. In algemene zin draait feedback om “teruggekoppelde informatie over de mate waarin het systeem zijn doelstellingen bereikt” (Remmerswaal, 2015). Andere termen die worden gebruikt voor dit circulaire proces zijn ‘cybernetische controle-lus’, ‘digitale controle-loop’ en ‘AI-levenscyclus’ (Kaufman, 2024; Schuilenburg, 2024). Hoe verschillend deze termen ook zijn, ze delen het kenmerk dat er sprake is van een continue zelfregulering die door verschillende stadia heenloopt – en weer terug.

Aan de hand van de term ‘AI-levenscyclus’ kunnen de verschillende stadia van datagedreven werk beter worden begrepen en het begrip ‘feedback’ handen en voeten worden gegeven zodat het niet als nat zeep uit onze handen glipt. Hiertoe is het instructief om de verschillende stadia van een AI-levenscyclus onder te verdelen in *input*, *throughput* en *output* (WRR, 2016; Peeters & Schuilenburg, 2023; Wessels, 2023; Schuilenburg, 2024). Deze drie stadia werken voortdurend in elkaar door en zullen dus altijd in hun samenhang moeten worden bekeken. Om van inputdata via throughput tot outputdata te komen, kunnen de volgende concrete stappen worden onderscheiden in datagedreven politiewerk (o.a. Van de Sandt et al., 2021; Hirsch et al., 2023; Landman, 2023):

- Verzamelen (*input*): het vergaren van data. Het kan hierbij onder meer gaan over *found data* (data die verzameld zijn door een passief, niet-observationeel dataverzamelingsproces) of *automated data* (data die automatisch worden gegenereerd door surveillance-apparaten en systemen van de politie) (Snaphaan & Hardyns, 2021). Ook is het mogelijk dat de politie datasets koopt van private partijen. Dit worden ‘niet-politionele data’ (Brayne, 2017) genoemd en deze data kunnen komen van sociale media (Facebook, X, Instagram), apps (Google Street View, Waze navigatie), slimme apparaten (iRobot vacuümstofzuiger, intelligente koelkast) of sensoren die op het lichaam worden gedragen (Apple Watch, Fitbit, Ray-Ban Stories bril) of zijn

⁴ In *Making Information Matter* voegt Kaufman (2024) hieraan het stadium toe van ‘imaginaries’ en stelt dat voordat het proces van verzamelen, analyseren en toepassen aanvangt er al sprake is van een vorm van ‘verbeelding’. Kaufman schrijft: “Data moeten als data worden verbeeld om als zodanig te kunnen bestaan en functioneren” (2024: 31). In de woorden van Dalton en Thatcher (2014): “Alle datasets zijn noodzakelijkerwijs beperkte representaties van de wereld die als zodanig moeten worden verbeeld om de betekenis te produceren die ze beweren te laten zien.”

bevestigd op objecten als toegangspoortjes, woningen (Amazon Ring deurbel) en auto's (Tesla) (Schuilenburg, 2024).

- Verwerking (*throughput*): het opslaan en bewerken van inputdata door middel van geautomatiseerd doorzoeken, ordenen, analyseren of in verband te brengen met reeds bekende gegevens waardoor relevante informatie (outputdata) ontstaat die vervolgens kan worden gebruikt in de opsporing.
- Intervenieren (*output*): het toepassen van interventies in de vorm van een concrete beslissing of een aanbeveling op basis van de geanalyseerde inputdata.

3. Juridische vraagstukken

Om een beter begrip te krijgen van de juridische vraagstukken op het gebied van datagedreven politiewerk is het instructief het hierboven gemaakte onderscheid aan te houden van *input*-, *throughput*- en *output* van een AI-toepassing. Hierbij moet worden aangetekend dat in de praktijk een strikt onderscheid tussen deze drie stadia lastig is te maken; het onderscheid is vooral instructief bedoeld om zo een tentatief overzicht te bieden van de belangrijkste juridische vraagstukken bij de toepassing van AI ten behoeve van de strafvordering. In het navolgende geef ik op hoofdlijnen een bespreking van de juridische vraagstukken die in ieder van deze drie stadia spelen, te beginnen met de *input*.

3.1 Input

Het vraagstuk van datakwaliteit begint bij de *input* van een AI-toepassing: de data zelf. Snaphaan en Hardyns schrijven dat “data zowel intrinsiek als vanwege hun invloed op (lerende) algoritmen een effect hebben op de uitkomsten” (2021: 64). Datakwaliteit vertrekt vanuit de veronderstelling dat de data een accurate weerspiegeling zijn van de ‘echte’ wereld. Verschillende wetenschappers hebben erop gewezen dat in de praktijk dit zelden het geval zal zijn. Data zijn sociale constructies en daarbij spelen verschillende dimensies een rol: (1) nauwkeurigheid; (2) volledigheid; (3) betrouwbaarheid van bronnen; (4) tijdelijkheid; en (5) toegankelijkheid (Leese, 2022; 2024). Volledigheid bijvoorbeeld is een belangrijk probleem in de opsporing en handhaving van strafbare delicten omdat er altijd data zullen ontbreken rondom verdachte personen of criminele fenomenen. Toegankelijkheid gaat in dit verband over de vraag of data direct beschikbaar zijn of dat ze binnen een redelijk tijdsbestek beschikbaar kunnen worden gesteld. Leese wijst erop dat “in de politiecontext het vaak niet zozeer de vraag is of data over een bepaalde persoon, netwerk of gebeurtenis bestaan, maar of ze toegankelijk zijn en gebruikt kunnen worden” (2024: 35).

De *input* van een AI-toepassing vormt het vertrekpunt voor de interventie in de strafvorderlijke context, maar ook in de context van het inlichtingenwerk of bij de advisering aan de strafrechter, en daarbij kunnen data die zelf onjuist zijn, leiden tot een *output* in de vorm van beslissingen of aanbevelingen die ook problematisch zijn. Dit probleem staat in de literatuur bekend als het belang van zogeheten ‘schone data’ voor strafvorderlijke doeleinden (Richardson et al., 2019; Das & Schuilenburg, 2020). Voor alle datasystemen geldt namelijk: ‘Garbage in, garbage out’, een uitdrukking die wordt gebruikt om duidelijk te maken dat wanneer er vuile data in de analyses komen, de uitkomst ook vervuild zal zijn (Kilkenny & Robinson, 2018). Om die reden stelt de

AI-Act (art. 10) verregaande verplichtingen aan de zorg voor een hoge kwaliteit van de inputdata om het risico op discriminerende uitkomsten tot een minimum te beperken.

Datakwaliteit van een AI-toepassing wordt enerzijds beïnvloed door ‘onjuiste’ data, van onnauwkeurige data tot onbetrouwbaarheid van bronnen. Anderzijds kan er sprake zijn van data die ‘onrechtmatig’ zijn – en daarmee ook ‘vuil’ zijn. In het geval van onrechtmatige data gaat het om een schending van juridische regels bij het verkrijgen van de data, zoals in het geval van schending van normen in het Wetboek van Strafvordering of verdragsbepalingen van het EVRM. Hierbij kan worden gedacht aan data die komen uit of zijn afgeleid van bevooroordeelde of strafbare praktijken, zoals discriminatie of het plegen van (niet strikt noodzakelijk) geweld door politieagenten bij identiteitscontroles, fouilleringen of aanhoudingen (Schalkwijk, 2025). Ook kan hierbij worden gedacht aan het onrechtmatig toegang krijgen tot data uit allerlei inbeslaggenomen gegevensdragers, waaronder mobiele telefoons en computers (zie het arrest CG/Landek – Hof van Justitie EU 4 oktober 2024 in zaak C-548/21).

Het uitgangspunt van de strafvorderlijke rechtsbescherming is dat burgers moeten worden beschermd tegen beide soorten van vervuiling in AI-toepassingen die worden gebruikt door de politie. Dit volgt uit het feit dat het overheidsoptreden vanaf de eerste acties van de politie rechtmatig moet zijn. In theorie zijn er twee filters om vuile data te weren uit de *input* van AI-toepassingen: aan de voorkant en aan de achterkant van een AI-levenscyclus (Das & Schuilenburg, 2020). In het geval van de voorkant kan onder andere worden gedacht aan de taak van verwerkingsverantwoordelijke personen binnen de politie – privacyfunctionarissen, beleidsmedewerkers of ICT-experts – om vuile data te identificeren en te verwijderen uit de gebruikte datasets. In het geval van de achterkant van een AI-levenscyclus is het aan de strafrechter om te oordelen dat de opsporingsautoriteiten onrechtmatig verkregen of onjuiste data hebben gebruikt in een dataset. Zo kan de strafrechter op zitting de rechtmatigheid van opsporingsbevoegdheden toetsen, inclusief het gebruik van vuile data in de datasets die hebben geleid tot bewijs van een delict in een strafzaak.

Kijken we naar de vraag of met beide filters vuile data ook daadwerkelijk kunnen worden geweerd uit de datasets van de politie, dan moet worden geconstateerd dat deze ‘onvoldoende transparant en fijnmazig zijn om een effectieve bescherming tegen vuile data te kunnen bieden’ (Das & Schuilenburg, 2020: 264). Het risico dat vuile data blijven doorwerken in data-analyses van de politie blijft daarom aanwezig. Daarmee ben ik beland bij de *throughput*, de verwerking door algoritmes die inputdata omzet in outputdata, dikwijls in combinatie met domeinkennis en reeds bekende informatie.

3.2 Throughput

In het stadium *throughput* gaat het om de vraag of het werkproces zelf legitiem is. In het geval van de dataverwerking door een AI-toepassing in het kader van strafvorderlijke doeleinden hebben verschillende auteurs gewezen op juridische onduidelijkheden met betrekking tot (i) de relatie tussen verzamelen en verwerken van data en (ii) het onafhankelijke toezicht hierop (o.a. Schermer, 20217; Commissie-Koops, 2018; Fedorova et al., 2022; Hirsch Ballin & Oerlemans, 2023). Zo stelt de Commissie-Koops in het rapport *Regulering van opsporingsbevoegdheden in een digitale omgeving* dat met betrekking tot het verzamelen en verwerken van data ‘een integrale visie’ (2018: 25)

ontbreekt met betrekking tot de normering van de dataverwerking, alsmede dat er een regeling dient te komen over ‘de inrichting van extern toezicht’ (2018: 31) op de dataverwerking en -verwerking door opsporingsdiensten. Met betrekking tot de wisselwerking tussen verzamelen en verwerken van data is het volgende van belang.

Hiervoor is gesteld dat in toenemende mate AI-toepassingen worden gebruikt door de politie waardoor de politie de beschikking krijgt over grote hoeveelheden data, van het onderscheppen van cryptocommunicatiedata van de door criminele organisaties gebruikte chatdienst EncroChat tot de inzet van realtime intelligence (denk bijvoorbeeld aan automatische kentekenplaatherkenning) in de opsporing. Een aandachtspunt is dat de activiteiten van het verzamelen en verwerken van de vergaarde data zich in de praktijk lastig laten scheiden, zoals in het geval van de bevoegdheid tot binnendringen in een gegevensdrager zoals een smartphone waarbij ook allerlei verwerkingshandelingen moeten worden verricht om de vergaarde gegevens voor de opsporing van strafbare feiten te kunnen gebruiken. In het Nederlandse juridische kader bestaat hierbij een spanning tussen twee wetten: de Wet Politiegegevens (Wpg) en het Wetboek van Strafvordering (WvSv).

In tegenstelling tot het WvSv (en de Politiewet), waarin voornamelijk de ‘verzameling’ van gegevens is geregeld ten behoeve van lopend onderzoek, biedt de Wpg een meer algemeen kader wat betreft de normering van de ‘verwerking’ en ‘analyse’ ervan (Van Schendel & Cuijpers, 2023). Fedorova et al. (2022) wijzen in het rapport *Strafvorderlijke gegevensverwerking* op de implicaties van een separate normering. Zo is de Wpg primair bedoeld om een zorgvuldige omgang met gegevens te waarborgen en niet om de opsporing te normeren – dat gebeurt in het WvS. Fedorova et al. schrijven: “Waar het in strafvordering gaat om het identificeren en bestraffen van de werkelijk schuldige aan een strafbare gedraging (en het vrijwaren van de onschuldige), is de verwerking van (vooralsnog) de politiegegevens voornamelijk ingegeven door het stroomlijnen van de gegevenshuishouding van het justitiële apparaat in het kader van een fatsoenlijke bescherming van de (individuele) privacybelangen” (2022: 4). Dit leidt tot de vraag hoe deze volledig verschillende activiteiten adequater juridisch genormeerd kunnen worden (zie ook: Schermer, 2022; Hirsch Ballin & Oerlemans, 2023).

De gescheiden juridische normering van verzamelen en verwerken van data heeft ook implicaties voor de toetsing of beoordeling ervan. Ook de toezichthoudende taak is in beide wetten anders belegd. In het WvSv zijn de rechter-commissaris en officier van justitie de partijen met een belangrijke toezichthoudende taak – en de toetsing door de strafrechter later. In de Wpg zijn de belangrijkste toezichthoudende taken neergelegd bij de privacyfunctionarissen binnen de politie (intern) en de Autoriteit Persoonsgegevens (extern) (Fedorova et al., 2022: 25). In het kader van toezicht op naleving van de wet door de Autoriteit Persoonsgegevens moet worden opgemerkt dat diens bevoegdheden zeer beperkt zijn, zo heeft de Autoriteit geen bevoegdheid om verwerkingen stil te leggen en zij kan ook geen onrechtmatig verwerkte gegevens zelf verwijderen (Stevens et al., 2021). Hirsch Ballin en Oerlemans (2023) pleiten daarom ervoor dat een keuze wordt gemaakt voor óf normering van data-analyses in het WvSv óf voor nadere normering van analysebevoegdheden in de Wpg.

3.3 Output

Het proces van *input* via *throughput* leidt uiteindelijk tot een concrete beslissing of een aanbeveling van een of meerdere acties in het kader van de strafvordering, gericht op een dader, slachtoffer of criminele infrastructuur (*output*). Zo kan de verwerking van data op grond van de Wpg leiden tot het aanleveren van bewijs van een delict in een strafzaak. Ook kan op basis van de uitkomsten van een AI-toepassing worden besloten meer politiemensen in te zetten op plaatsen waar schietincidenten of woninginbraken worden verwacht. In *Regulering van opsporingsbevoegdheden in een digitale omgeving* wijst de Commissie-Koops erop dat dit proces “bijzondere risico’s voor grondrechten van burgers en de integriteit van de opsporing met zich meebrengen; te denken valt aan de mogelijke gevolgen van vals-positieven en ongegronde aannames gebaseerd op ondoorzichtige algoritmische analyses” (2018: 26). In het laatste geval kan onder meer worden gedacht aan het voorspellen van criminaliteit door de Nationale Politie via het Criminaliteits Anticipatie Systeem (CAS) – een systeem dat in staat is om autonoom te leren en zelfstandig voorspellingen te genereren. Dataprofessionals die bij CAS betrokken waren, gaven aan dat “in combinatie met de grootte van de dataset en het hoge aantal voorspellingen, de interne beslissingslogica van voorspellingen in de praktijk ondoorzichtig was” (Waardenburg, 2021: 92).

In de literatuur wordt erop gewezen dat voor geautomatiseerde data-analyses en besluitvorming een explicitering van de eis van uitlegbaarheid in het WvSv wenselijk is. Zo dienen onder meer beslissingen in het vooronderzoek deugdelijk gemotiveerd (en dus controleerbaar) te zijn. Dit begint al bij de verdenking van een strafbaar feit. Strafvorderlijke beslissingen moeten altijd uitlegbaar – in de zin van gemotiveerd – te zijn, maar in het geval van beslissingen die zijn gebaseerd op geavanceerde en geautomatiseerde data-analyses dreigt het risico op “niet specifiek gemotiveerde, en daarmee moeilijk weerlegbare, beslissingen: ‘system says so’” (Commissie-Koops, 2018: 28).

In het kader van datagedreven politiewerk is het recht van de ‘equality of arms’ uit artikel 6 EVRM relevant. Op basis van dit recht moeten de verdachte en verdediging de mogelijkheid krijgen het voor de zaak relevante materiaal te bestuderen en daarop te reageren – en daarvoor zijn voldoende tijd, gelegenheid of middelen noodzakelijk (Egberts, 2022). Hierbij kan volgens Schermer en Oerlemans (2020) worden gedacht aan de inrichting van een *data room* waar de verdachte en verdediging een dataset relatief eenvoudig kunnen bevragen. De eerste stappen hiertoe zijn reeds gezet door het Nederlands Forensisch Instituut met een methode waarmee advocaten via de digitale zoekmachine Hansken vanaf hun eigen kantoor cryptocommunicatie kunnen inzien. Kennis van de technische kant van AI-toepassingen is hiervoor wel noodzakelijk. Zo stelt de WRR in haar rapport *Opgave AI: “Inzage betekent nog geen inzicht”* (2021: 116); een probleem wat vooral speelt bij algoritmes die werken op basis van *machine learning* en dus zelf een weg zoeken door de datasets heen (Schuilenburg & Peeters, 2024). Deze algoritmes gaan verder dan klassieke ‘rule-based’ algoritmes en kunnen leiden tot allerlei onverwachte statistische verbanden, die niet altijd verklaarbaar of aantoonbaar causaal zijn (Custers, 2016; 2023).

4. Conclusie en discussie

Het gebruik van AI-toepassingen door de politie zal de komende jaren in een stroomversnelling komen. Dit leidt tot een intensivering van zowel de omvang als de diepgang van manieren van opsporing en handhaving van criminaliteit, van biometrische gezichtsherkenning en het detecteren van levensbedreigende boodschappen in online tekstberichten (*Threat To Life*-model) tot het snelgroeende terrein van geografische en persoonsgebonden criminaliteitsvoorspelling. Het is daarom noodzakelijk om het debat over het heden en de toekomst van AI met betrekking tot datagedreven politiewerk breder te voeren dan tot nu toe gebeurt. Juridische vragen over het recht op privacy of discriminatie van minderheden bijvoorbeeld bestaan al langer, maar de huidige ontwikkelingen met betrekking tot de inzet van AI-toepassingen vereisen meer aandacht omdat het gebruik ervan tal van risico's met zich meebrengt voor fundamentele mensenrechten, met name wanneer de data-analyses complexer worden door zelflerende algoritmes (Glaser et al., 2021; Schuilenburg & Soudijn, 2023). Het is daarom noodzakelijk dat er voldoende juridische waarborgen zijn voor deze risico's. Daarbij is het belangrijk voor ogen te houden dat AI altijd iets voorlopigs in zich heeft en uiteindelijk ook iets ambivalents: ze biedt oplossingen en creëert tegelijk problemen.

Ik heb me in dit artikel gericht op de juridische problematiek rondom de levenscyclus van een AI-toepassing op het gebied van de strafvordering. Aan de hand van het begrip 'AI-levenscyclus' is een onderscheid gemaakt tussen drie stadia van een AI-tool: *input*, *throughput* en *output*. Door de drie stadia te bezien van het idee van een levenscyclus is duidelijk waarom ze in elkaar blijven doorwerken en dus voortdurend van invloed zijn op elkaar. Opmerkelijk is dat het huidige juridische debat over AI-toepassingen zich vooral richt op de verwerking van data (*throughput*). Hierdoor bestaat het gevaar dat er onvoldoende aandacht is voor zowel de *input* als de *output* alsmede voor de feedbackprocessen tussen de drie stadia.

In deze bijdrage is in ieder stadium gekeken naar relevante juridische vraagstukken op het gebied van de strafvordering. Dit betreft uiteindelijk een niet-uitputtende opsomming, waarbij onder meer is gewezen op het risico van vuile data in de datasets (*input*) en de (on)mogelijkheden van het inzagerecht en 'equality of arms' bij het gebruik van grote hoeveelheden data door de politie (*output*). Daarbij zijn ook oplossingsrichtingen aan bod gekomen voor de geconstateerde juridische kwesties, waaronder het inrichten van een *data room*, een beveiligde ruimte waarin de verdachte en verdediging toegang krijgen tot de datasets die vertrouwelijke informatie bevatten ten behoeve van de opsporing van strafbare delicten. Naast inzage in de datasets, krijgt de verdediging bij de start van de *data room* dan ook uitleg over de AI-toepassing en de gebruikte algoritmes. Een andere oplossing is het presenteren van een 'chain of evidence' door de politie en het Openbaar Ministerie bij het nemen van beslissingen in de opsporing en vervolging van strafbare feiten. Een 'chain of evidence' moet dan onder andere duidelijk maken met welke inputdata is gewerkt en wat er met die data is gebeurd. De handelingen die met de data zijn uitgevoerd, dienen hierbij voortdurend vast te worden gelegd door de opsporingsinstanties.

Een beperking van de indeling in drie stadia van een AI-toepassing is dat er geen aandacht is voor de *outcome*. In termen van het concept van een AI-levenscyclus: het 'leven' zelf waardoor data materieel worden. Bij *outcome* gaat het niet alleen om de

instrumentele vraag of er een effect is op de criminaliteit (daling of stijging), maar ook om de vraag ‘waarom en onder welke omstandigheden’ een AI-toepassing wel of niet werkt en in ‘welke normatieve context’ een AI-toepassing wordt ingezet.⁵ Dit betekent dat onder meer moet worden gekeken of in de praktijk de bedoeling met de interventies ook dichterbij is gebracht. Het veilig maken van de samenleving (‘securitisering’) dient zowel zorgvuldig en correct tot stand te komen als efficiënt te zijn – en dan “niet alleen in termen van *output* (het halen van de doelen), maar ook in termen van *outcome* (het bereiken van bredere maatschappelijke opbrengsten)” (Van der Steen, 2024: 26).

Daarnaast is er nog een andere kant van een AI-toepassing die onbenoemd is gelaten en dat is de kwestie dat de professional wordt gezien als ultieme tegenwicht voor geavanceerde en geautomatiseerde data-analyses. Hiermee keer ik terug naar het begin van het artikel dat de digitalisering en algoritmisering van het politiewerk een socio-technologische opgave is. Net als de eerder geconstateerde juridische zorgen over de kwaliteit van de data en de gevolgen hiervan voor de opsporing van strafbare delicten, moet niet worden vergeten dat ook politieprofessionals onbewuste vooroordelen kunnen hebben op basis waarvan ze handelen in concrete situaties en beslissingen nemen. In dit verband wijzen gedragswetenschappers onder andere op de neiging van personen om intenties toe te schrijven aan gebeurtenissen (*intentionality bias*) en de aandrang om informatie te zoeken en te selecteren die bestaande overtuigingen ondersteunt en tegelijk minder aandacht te hebben voor informatie die deze tegensprekt (*confirmation bias*) (Lidén, 2023). Hierdoor kunnen ook verkeerde besluiten worden genomen: ‘een bias blijft met andere woorden een bias, ook als de tekortkomingen van de technologie menselijk moeten worden opgelost’ (Schuilenburg, 2024: 110).

Nauw hiermee samenhangt dat elke vorm van besturen uiteindelijk altijd disciplineert. Hiermee bedoel ik dat de inzichten van Max Weber (bureaucratie) en Michel Foucault (discipline) ook opgaan in een ‘data-level bureaucratie’ (Schuilenburg & Peeters, 2024) waarbij de uitkomsten van een algoritme de rationalisatie zijn geworden achter de besluitvorming van publieke organisaties. Zelfs met getrainde specialisten ‘in the loop’ kan het zo zijn dat politieprofessionals juist willen vluchten in een algocratische manier van besturen. Er zijn namelijk tal van redenen om de uitkomsten van algoritmes wel over te nemen en de aanbeveling of de beslissing na te leven die door de AI-toepassing wordt voorgesteld. Zo biedt naleving een zekere mate van bescherming en veiligheid om beslissingen te kunnen legitimeren. In de bestuurskunde wordt hierbij gesproken van ‘potentiële verantwoording’, waarbij achteraf verantwoording kan worden afgelegd bij misstanden of calamiteiten door de algoritmische modellen hiervan de schuld te geven (Noordegraaf & Sterrenburg, 2009). In het verlengde hiervan is gewezen op het fenomeen ‘machine justice’ (Peeters & Schuilenburg, 2018) en daarbij op de paradox dat zelflerende algoritmes de suggestie wekken dat het besluitvormingsproces constant in beweging is, maar het gebruik ervan juist kan leiden tot digitale rigiditeit – het strikt en gedisciplineerd naleven van de uitkomsten van een AI-toepassing.

⁵ Zo wordt het politieke vertoog gedomineerd door een streven naar meer veiligheid met een brede steun om risico’s in een zo vroeg mogelijk stadium te voorkomen (Schuilenburg & Van Swaaningen, 2013). Tel hierbij het geloof op dat alles is te vatten in data (ook wel ‘dataficatie’ genoemd) en dat veiligheidsproblemen effectiever met de nieuwste technologische tools kunnen worden aangepakt, en dit alles resulteert in een groot geloof in AI en algoritmes als ‘de’ oplossing voor het veiligheidsvraagstuk (Morozov, 2013; Aradau, 2023) – ook wel ‘AI-ism’ genoemd.

Kortom, een socio-technologische benadering van datagedreven politiewerk vraagt om inzicht in datgene wat AI allemaal kan doen voor de politie, maar ook wat AI allemaal met de politieprofessional doet.

Bibliografie

- AFZAL, M. & P. PANAGIOTOPOULOS (2024). Data in Policing: An Integrative Review. *International Journal of Public Administration*, 1–20.
- ARADAU, C. (2023). Borders have always been artificial: Migration, data and AI, *International Migration*, 61, 303–306.
- BELLANOVA, R. (2025). Databases. In: M. Kaufmann & H.M. Lomell (eds.), *De Gruyter Handbook of Digital Criminology*, Berlin: Walter de Gruyter, 173–180.
- BENJAMIN, R. (2019). *Race After Technology: Abolitionist Tools for the New Jim Code*, Medford, MA: Polity Press.
- BENNETT MOSES L. & J. CHAN (2018). Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 28(7), 806–822.
- BRAYNE, S. (2017). Big Data Surveillance: ‘The Case of Policing’, *American Sociological Review*, 82(5), 977–1008.
- COMMISSIE-KOOPS (2018). *Reguleren van opsporingsbevoegdheden in een digitale omgeving*, Den Haag.
- CUSTERS, B. (2016). Big Data in Wetenschappelijk Onderzoek, *Justitiële Verkenningen*, 1, 8–21.
- CUSTERS B. (2023). Technologiekennis voor een eerlijk proces: fair trial vereist ook van rechters enige kennis van complexe technologie, *Nederlands Juristenblad*, 98(21), 1733–1741.
- DALTON, C. & J. THATCHER (2014). What Does a Critical Data Studies Look Like, and Why Do We Care?, <http://societyandspace.org/2014/05/12/what-does-a-critical-data-studies-look-like-and-why-do-we-care-craig-dalton-and-jim-thatcher/> (geraadpleegd: 18 maart 2025).
- DAS, A. & M. SCHUILENBURG (2020). Garbage in, garbage out: Over predictive policing en vuile data, *Beleid en Maatschappij*, 47(3), 254–268.
- DOURISH, P. & E. GÓMEZ CRUZ (2018). Datafication and Data Fiction: Narrating Data and Narrating with Data, *Big Data & Society*, 5(2), 1–10.
- EGBERTS, M.M. (2022). De reikwijdte van het inzagerecht en ‘equality of arms’ in het licht van grote datasets, Hansken en toekomstige ontwikkelingen. *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 8(2), 119–129.
- ENARSSON, T., ENQVIST, L., & M. NAARTTIJÄRVI (2021). Approaching the human in the loop – legal perspectives on hybrid human/algorithmic decision-making in three contexts. *Information & Communications Technology Law*, 31(1), 123–153.
- FEDOROVA, M.I., R.M. TE MOLDER, M.J. DUBELAAR, S.M.A. LESTRADE & T.F. WALREE (2022). *Strafvorderlijke gegevensverwerking. Een verkennende studie naar de relevante gezichtspunten bij de normering van het verwerken van persoonsgegevens voor strafvorderlijke doeleinden*, Nijmegen: Radboud University Press.
- FERGUSON, A.G. (2017). *The Rise of Big Data Policing. Surveillance, Race, and the Future of Law Enforcement*, New York: NUY-Press.
- GLASER V.L., N. POLLOCK, & L. D’ADDERIO (2021). The Biography of an Algorithm: Performing algorithmic technologies in organizations, *Organization Theory*, 2(2), doi.org/10.1177/26317877211004609.
- HADJIMATHEOU, K. & P. FUSSEY (2025). ‘The dream to know everything about everyone’: Affordances of commercial data systems and digital net-widening in policing. *Theoretical Criminology*, 29(3), 325–345.
- HARDYNS, W. & A. RUMMENS (2017). Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges, *European Journal on Criminal Policy and Research*, 24, 201–218.
- HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (2019). *Ethics guidelines for trustworthy AI*, Brussels: European Commission.
- HIRSCH BALLIN, M.F.H. & J.J. OERLEMANS (2023). Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden, *Delikt en Delinkwent*, 1(2), 18–38.
- JOHNSTON, J. (2008). *The Allure of Machinic Life: Cybernetics, Artificial Life, and the New AI*. Boston: MIT Press.
- KATZ, Y. (2020). *Artificial Whiteness: Politics and Ideology in Artificial Intelligence*, New York: Columbia University Press.

- KAUFMANN, M. (2024). *Making Information Matter: Understanding Surveillance and Making a Difference*, Bristol: Bristol University Press.
- KHALFA, R., T. SNAPHAAN, O. WIJSMAN ET AL. (2024). Big data policing: de implicaties van digitalisering en maatschappelijke dataficatie voor de politiefunctie en het politiewerk, *Tijdschrift voor Veiligheid*, (23)1-2, 31-52.
- KILKENNY, M.F. & K.M. ROBINSON (2018). Data quality: "Garbage in – garbage out", *Health Information Management Journal*, 47(3), 103-105.
- KITCHIN, R. (2025). *Critical Data Studies: An A to Z Guide to Concepts and Methods*, Cambridge: Polity Books.
- KITCHIN, R., J. DAVRET, C.M. KAYANAN & S. MUTTER (2025). Data mobilities: Rethinking the movement and circulation of digital data, *Mobilities*, 1-19.
- LANDMAN, W. & S. GROOTHUIS (2022). *Politiewerk op het web. Een verkennend onderzoek naar online gegevensvergaring door de politie*, Den Haag: Sdu Uitgevers.
- LANDMAN, W. (2023). *Politiewerk aan de horizon. Technologie, criminaliteit en de toekomst van politiewerk*. Den Haag: Sdu Uitgevers.
- LATOUR, B. (1993). *We Have Never Been Modern*, Cambridge: Harvard University Press.
- LATOUR, B. (2005). *Reassembling the Social. An Introduction to Actor-Network Theory*, Oxford: Oxford University Press.
- LEESE, M. (2022). Data quality in governance: A definition and a research agenda, CURATE Working Paper 1, doi.org/10.3929/ethz-b-000581434 (geraadpleegd: 12 maart 2025).
- LEESE, M. (2024). Data Quality in Police Work. In: Kuldova, T.Ø., Gundhus, H.O.I. & C.T. Wathne (eds.), *Policing and Intelligence in the Global Big Data Era*, Volume II. Palgrave's Critical Policing Studies. Cham: Palgrave Macmillan, 25-47.
- LEONELLI, S. (2020). Learning from Data Journeys. In: Leonelli, S. & N. Tempini (eds.), *Data Journeys in the Sciences*, Cham: Springer Open, 1-26.
- LIDÉN, M. (2023). *Confirmation Bias in Criminal Cases*, Oxford: Oxford University Press.
- M McNALLY, R., A. MACKENZIE, A. HUI & J. TOMOMITSU (2012). Understanding the 'Intensive' in 'Data Intensive Research': Data Flows in Next Generation Sequencing and Environmental Networked Sensors, *International Journal of Digital Curation*, 7(1), 81-94.
- MOROZOV, E. (2013). *To save everything, click here*, New York: Public Affairs Books.
- NATIONALE POLITIE (2025). *Stevig staan in deze tijd: Strategische agenda politie 2025-2030*, Den Haag.
- PARLEMENTAIRE ENQUÊTECOMMISSIE FRAUDEBELEID EN DIENSTVERLENING (2024). *Blind voor mens en recht*. Den Haag: Tweede Kamer der Staten-Generaal.
- PEETERS, R. & M. SCHUILENBURG (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.
- PEETERS, R. & M. SCHUILENBURG (2023). Algorithmic Governance: Technology, Power, and Knowledge. In: Housley, W., Edwards, A., Beneito-Montagut, R. & R. Fitzgerald (eds.), *The SAGE Handbook of Digital Society*, London: Sage, 439-457.
- REMMERSWAAL, J. (2015). Feedback. In: *Begeleiden van groepen*. Houten: Bohn Stafleu van Loghum, https://doi.org/10.1007/978-90-368-0725-8_10.
- RICHARDSON, R., J. SCHULTZ & K. CRAWFORD (2019). Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice, *New York University Law Review Online*, 94(192), 192-233.
- SCHALKWIJK, J. (2025). De beoordeling van politiegeweld in Nederland, *Nederlands Juristenblad*, 480(9), 659-665.
- SCHERMER, B.W. (2017). Het gebruik van Big Data voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens, *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 4, 207-216.
- SCHERMER, B.W. & J.J. OERLEMANS (2020). AI, strafrecht en het recht op een eerlijk proces, *Computerrecht*, 3(1), 14-21.
- SCHUILENBURG, M. (2016). Predictive policing: De opkomst van een gedachtenpolitie?, *Ars Aequi*, (65)12, 931-936.
- SCHUILENBURG, M. & M. SOUDIYN (2023). Big Data Policing: The Use of Big Data and Algorithms by the Netherlands Police, *Policing: A Journal of Policy and Practice*, 17, paado61.
- SCHUILENBURG, M. (2024). *Making Surveillance Public: Why You Should Be More Woke about AI and Algorithms*. The Hague: Eleven International Publishing.

- SCHUILENBURG, M. (2025). Technologie is nooit neutraal: Over het publiek maken van AI en algoritmes. In: R. de Brabander (ed.), *Bouwen aan vertrouwen: Sociaal professionals tussen burgers en overheid*, Assen: Van Gorcum, *forthcoming*.
- SCHUILENBURG, M. & R. PEETERS (2024). Voorbij de system-level bureaucratie: Over datastromen, algoritmes en inclusieve AI in de databureaucratie, *Beleid en Maatschappij*, (51)3, 278-293.
- SCHUILENBURG, M. & R. VAN SWANINGEN (2013), Veiligheid in een laatmoderne cultuur, *Tijdschrift over Cultuur & Criminaliteit*, (3)2, 109-122.
- SNAPHAAN, T. & W. HARDYNS (2021). Handvatten voor een kwaliteitsbeoordeling van big data: De introductie van het Total Error raamwerk, *Tijdschrift voor Veiligheid*, (20)4, 63-88.
- STEVENS, L., M. HIRSCH BALLIN, M. GALIČ ET AL. (2021). Strafvorderlijke normering van preventief optreden op basis van datakoppeling, *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 4, 234-245.
- TERPSTRA, J. & R. SALET (2020). Big data policing als sociale praktijk: Schets van een miskend, maar urgent onderzoeksterrein, *Cahiers Politiestudies*, 54, 25-38.
- VAN BRAKEL, R. (2023). Artificiële Intelligentie en veiligheid: Kansen en uitdagingen, *Politie & Recht*, 4, 151-162.
- VAN BRAKEL, R. & L. GOVAERTS (2024). Exploring the impact of algorithmic policing on social justice: Developing a framework for rhizomatic harm in the pre-crime society, *Theoretical Criminology*, 29(1), 91-109.
- VAN DE SANDT, E. A. VAN BUNNINGEN, J. VAN LENTHE & J. FOKKER (2021). Towards Data Scientific Investigations: A Comprehensive Data Science Framework and Case Study for Investigating Organized Crime and Serving the Public Interest, paper presented at the Third INTERPOL-UNICRI Global Meeting on AI for Law Enforcement, 25 November 2020, REPHRAIN.
- VAN SCHENDEL, S. & C. CUIJPERS (2023). Bigdatatoepassingen in de opsporing: Een pleidooi voor de integratie van fundamentele mensenrechtenbescherming in het strafprocesrecht, *Cahiers Politiestudies*, 66, 135-150.
- VAN DER STEEN, M. (2024). *Technologie in de tussentijd: AI, publieke waarde en democratie*, Den Haag: NSOB.
- WAARDENBURG, L. (2021). *Behind the scenes of artificial intelligence: Studying how organizations cope with machine learning in practice*, Alblasterdam: Haveka.
- WESSELS, M. (2023). Accountability of Algorithmic Policing: Eight Sociotechnical Challenges, *Policing and Society*, 34(3), 124-138.
- WRR (2016). *Big Data in een vrije en veilige samenleving*, Amsterdam: Amsterdam University Press.
- WRR (2023). *Opgave AI: De nieuwe systeemtechnologie*, Den Haag.