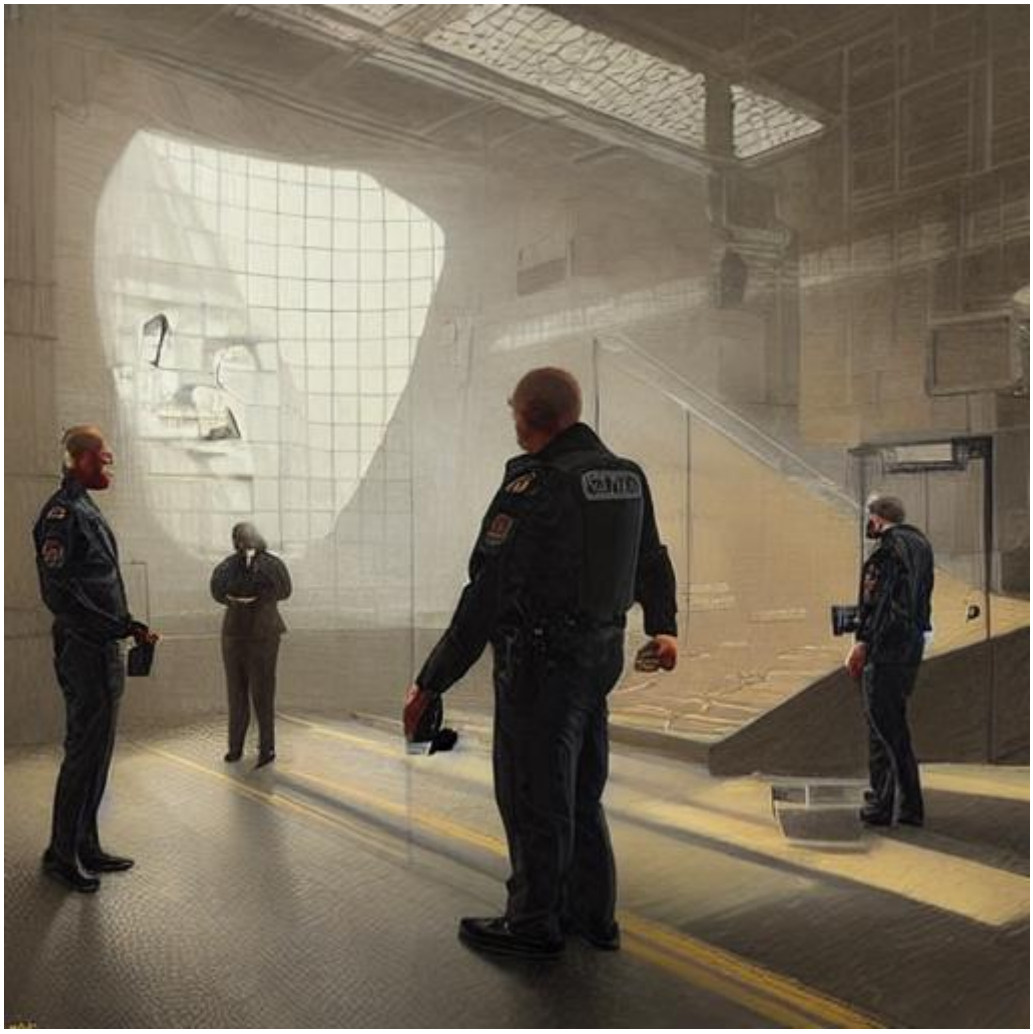
Kunstmatige intelligentie bij de politie

Een internationale literatuurstudie



Dr. **Dennis de Kool** (Erasmus Universiteit Rotterdam/Risbo)
Dr. **Brenda Vermeeren** (Erasmus Universiteit Rotterdam /ESSB)
Prof.dr. **Bram Steijn** (Erasmus Universiteit Rotterdam /ESSB)

Opdrachtgever: Politie en Wetenschap

-Definitieve versie augustus 2023-

Inhoudsopgave

Samenvatting

Kunstmatige intelligentie (hierna te noemen: AI) wordt beschouwd als één van de belangrijkste strategische technologieën van deze eeuw en één van de sleuteltechnologieën in de digitale transitie. Dit is een belangrijke aanleiding geweest om een internationale literatuurstudie uit te voeren op het gebied van AI bij de politie. De tussentijdse bevindingen zijn periodiek voorgelegd aan een begeleidingscommissie en andere kritische tegenlezers binnen de politie om de validiteit te vergroten.

In de literatuur is er (nog) geen eenduidige en gezaghebbende definitie van AI. Iedere definitie roept discussie op. In deze literatuurstudie is de volgende werkdefinitie van kunstmatige intelligentie gehanteerd: “artificial intelligence refers to systems that display intelligent behavior by analyzing their environment and taking actions – with some degree of autonomy – to achieve specific goals.”

De doelstelling die in dit onderzoek centraal gestaan heeft, is om op basis van internationale literatuur (empirische) inzichten te vergaren in de ervaringen die politieorganisaties in het buitenland opdoen met kunstmatige intelligentie en daar relevante inzichten en concrete aandachtspunten uit af te leiden. In het bijzonder is daarbij aandacht besteed aan kansen, risico’s en kritische succesfactoren voor de samenleving (macroniveau), de politieorganisatie (mesoniveau) en individuele burgers en politieprofessionals (microniveau). De ervaringen die de politie elders opdoet met AI kan de Nederlandse politie behulpzaam zijn bij het beredeneerd en effectief implementeren van AI-toepassingen.

Hierbij dient te worden opgemerkt dat positieve of negatieve ervaringen die de politie in het buitenland opdoet, dan wel heeft opgedaan met AI, niet per definitie relevant of bruikbaar zijn voor de Nederlandse politiepraktijk. Per land kan de context waarbinnen de politie opereert en functioneert variëren. In dat kader kan een onderscheid worden gemaakt tussen de interne context (bijvoorbeeld de specifieke politiecultuur), de maatschappelijke context, de politiek-bestuurlijke context en de bredere context van de veiligheidsketen.

De probleemstelling heeft geresulteerd in de volgende centrale vraagstelling: welke empirisch gefundeerde lessen kunnen worden getrokken uit de in de internationale literatuur belichte ervaringen die politieorganisaties in het buitenland opdoen of hebben opgedaan met de beoogde en gerealiseerde implementatie van concrete AI-toepassingen, en welke casuïstiek en concrete aandachtspunten kunnen op basis van deze internationale ervaringen worden aangereikt op basis waarvan de politie in Nederland AI effectief kan inzetten om haar doelen te bereiken?

Deze vraagstelling valt uiteen in vijf deelvragen:

1. Welke (verwachte) kansen van AI worden in de internationale politieliteratuur waargenomen?
2. Welke (verwachte) risico’s van AI worden in de internationale politieliteratuur waargenomen?
3. Welke kritische succesfactoren kunnen uit de vergelijking van de cases in de deskstudie worden gedestilleerd om AI effectief en succesvol in te zetten?
4. Welke rol speelt de interne context (politiecultuur), de maatschappelijke context, de politiek-bestuurlijke context, de juridische context en de bredere context van de veiligheidsketen bij de mogelijke inzet van AI?
5. Hoe kunnen de vergaarde empirische inzichten uit de internationale politieliteratuur in samenwerking met de Nederlandse politie worden vertaald naar concrete, beredeneerde en bruikbare aandachtspunten voor de (Nederlandse) politiepraktijk?

Deze literatuurstudie is gericht op het analyseren en bestuderen van wetenschappelijke publicaties over de toepassing van AI door de politie in het buitenland. Dit impliceert dat geen veldonderzoek is uitgevoerd en casuïstiek waarover (nog) niet is gepubliceerd, niet is meegenomen in de analyse. De analyse omvat drie niveaus, namelijk het macroniveau, het mesoniveau en het microniveau.

De internationale literatuur is verzameld met behulp van Google Scholar. De zoekperiode is afgebakend van januari 2011 tot en met het voorjaar 2022. Het zwaartepunt van de bestudeerde literatuur bestaat uit artikelen in wetenschappelijke tijdschriften. Een klein deel van de bestudeerde literatuur omvat hoofdstukken in geredigeerde boeken. Artikelen in vakbladen vallen daarmee buiten de focus. Bij de selectie van de relevante literatuur is tevens de 'sneeuwbalmethode' toegepast, waarbij op basis van de geïnventariseerde literatuur is gekeken naar welke wetenschappelijke publicaties (artikelen en boeken) wordt doorverwezen en welke trefwoorden in de bestudeerde literatuur zijn vermeld. Om relevante artikelen te vinden zijn verschillende losse en gecombineerde zoektermen gehanteerd (zie hoofdstuk 2).

In totaal zijn er ruim 175 publicaties bestudeerd. In de bestudeerde literatuur kan een onderscheid worden gemaakt tussen empirisch gefundeerde en beschouwende artikelen. Voor deze deskstudie zijn empirische artikelen het meest relevant, omdat deze inzicht bieden in de empirische ervaringen die politieorganisaties reeds hebben opgedaan. In de verschillende hoofdstukken zal echter blijken dat het aantal empirisch gefundeerde artikelen beperkt is in relatie tot beschouwende publicaties.

De bevindingen zijn geclusterd in drie hoofdstukken op basis van drie thematische clusters die in de bestudeerde internationale literatuur het vaakst zijn genoemd, namelijk predictive policing, smart policing en automated policing. Predictive policing komt er in het kort op neer dat de politie met behulp van slimme software historische data analyseert met als doel om mogelijke criminele gedragingen in de toekomst te voorspellen en daar op te anticiperen zodat criminele gedragingen voorkomen kunnen worden (zie hoofdstuk 3). Smart policing betreft het monitoren van verdachte activiteiten in de publieke ruimte of online, waarbij de politie gebruik kan maken van verschillende apparaten en toepassingen (zie hoofdstuk 4). Automated policing betreft het gebruik van robots en gerobotiseerde systemen bij de uitvoering van politietaken (zie hoofdstuk 5). Bij brede en abstracte concepten is iedere indeling arbitrair. Daar komt bij dat deze drie clusters elkaar niet uitsluiten. Toepassingen die minder goed te plaatsen waren binnen één van de genoemde clusters zijn in een separaat hoofdstuk beschreven en belicht onder het kopje 'overige toepassingen'.

Bevindingen

In de literatuur wordt AI op verschillende manieren gedefinieerd. Dat heeft ook zijn weerslag op dit onderzoek. Zowel in de begeleidingscommissie als tijdens de digitale focusgroep is er een semantische discussie gevoerd over de vraag wat AI precies is en welke toepassingen daar al dan niet onder geschaard kunnen worden. Deze literatuurstudie zal deze semantische discussie niet kunnen beslechten en dat is ook niet de insteek geweest. Een voortschrijdend inzicht is dat innovatie als begrip minder beladen is dan de term AI. Een ander voortschrijdend inzicht is dat de impact van AI uiteindelijk belangrijker is dan de aard ervan. In deze internationale literatuurstudie moet AI daarom niet worden benaderd als een dichotomie (wel of geen AI), maar als een schaal, waarbij de mate van intelligentie kan variëren van lage tot hoge intelligentie. De gedachte daarbij is dat hoe intelligenter AI is, des te zelfstandiger en autonomer de (politie)taken uitgevoerd kunnen worden.

Wanneer wordt gekeken naar de verhouding tussen empirisch gefundeerde en beschouwende artikelen, dan kan worden geconcludeerd dat de meeste artikelen die zijn bestudeerd een beschouwend karakter hebben en het aantal empirisch gefundeerde artikelen relatief beperkt is. Daar liggen verschillende mogelijke verklaringen aan ten grondslag. Een eerste verklaring is dat nog volop

ervaring wordt opgedaan door middel van pilots, proeftuinen en experimenten. De resultaten daarvan zijn veelal nog niet uitgekristalliseerd en belicht in wetenschappelijke literatuur. Een tweede verklaring is dat het bij de politie niet altijd gebruikelijk is om pilots en experimenten grondig te laten evalueren door externe (politie)onderzoekers. De lessen uit interne evaluaties zullen intern gedeeld worden, maar zijn niet altijd inzichtelijk voor de buitenwereld. Een derde verklaring die door politieonderzoekers naar voren werd gebracht, is dat transparantie op het gebied van AI bij de politie criminelen in de kaart kan spelen. De politie heeft er geen direct belang bij om ervaringen op het gebied van AI gedetailleerd te delen met (politie)onderzoekers. De politie in verschillende landen kan dus verder zijn in haar toepassing van AI dan de bestaande (wetenschappelijke) literatuur lijkt te suggereren. Daar komt bij dat het jaren kan duren voordat empirisch gefungeerde onderzoeken worden gepubliceerd in wetenschappelijke tijdschriften. Een alternatieve verklaring is dat de inzet van AI door de politie nog redelijk beperkt is, mede omdat AI nog volop in ontwikkeling is.

In dit onderzoek zijn verschillende onderzoeksvragen geformuleerd die hieronder beantwoord gaan worden.

Deelvraag 1: Wat zijn de (verwachte) kansen van AI voor de politie?

In de internationale literatuur wordt meer aandacht besteed aan de risico's (zie deelvraag 2) dan aan de kansen van AI. Een belangrijk en voor de hand liggend motief om AI-toepassingen in te zetten binnen politieorganisaties in het buitenland, is het verhogen van de veiligheid van de samenleving (macroniveau) en het verhogen van de effectiviteit en efficiency van de politieorganisatie (mesoniveau). Deze (verwachte) kansen spelen een rol bij predictive policing, smart policing & automated policing. De (verwachte) voordelen van kunstmatige intelligentie voor individuele politieprofessionals en individuele burgers wordt in de literatuur niet of nauwelijks belicht (microniveau). Een uitzondering vormen specifieke toepassingen op het gebied van automated policing, namelijk gerobotiseerde apparaten die gevaarlijk werk kunnen overnemen en daarmee het politiewerk veiliger kunnen maken voor individuele agenten (microniveau). Het veiliger maken van de samenleving heeft in dat opzicht ook een individuele dimensie. Voor wat betreft het verhogen van de effectiviteit, moet worden gedacht aan het voorspellende potentieel van AI. De effectiviteit van de politie kan door middel van predictive policing worden vergroot door locatiegerichte criminaliteit te voorspellen en daar gerichte interventies op te plegen, en door verdachte personen of situaties gericht in de gaten te houden. Smart surveillance kan gericht zijn op het monitoren van individuele personen. De inzet van AI ter verhoging van de efficiency omvat onder meer het inzetten van technologie, zodat de politie meer kan bereiken met minder menskracht. Bij automated policing wordt daarbij in de literatuur soms ook een individuele dimensie belicht: AI kan saaie en routinematige taken van politiemedewerkers overnemen, zodat zij hun tijd efficiënter kunnen benutten. In de literatuur wordt deze kans soms ook opgevat als een bedreiging. Daarvan is sprake wanneer de AI mensen vervangt en overbodig maakt. In de internationale literatuur zijn er geen concrete aanwijzingen dat dit laatste bij de politie het geval zou zijn. Kansen op microniveau worden weliswaar belicht in de internationale literatuur, maar minder frequent als de kansen op meso- en macroniveau.

Deelvraag 2: Wat zijn de (verwachte) risico's van AI voor de politie?

In het algemeen wordt in de internationale literatuur meer aandacht besteed aan de risico's dan de kansen van AI. Belangrijke (verwachte) generieke risico's die in de literatuur het vaakst zijn benoemd, hebben betrekking op discriminatie, privacy en de implicaties van fouten die AI-systemen kunnen maken.

Discriminatie kan onbedoeld optreden wanneer er sprake is van 'biases' in data of algoritmen die aan AI-systemen ten grondslag liggen. AI-systemen leren namelijk op basis van historische data en als er

'biases' in deze data zitten, dan liggen deze ook ten grondslag aan het leren van het systeem en dat is niet wenselijk. Een ander risico is dat de *privacy* van burgers wordt aangetast. Op het veiligheidsdomein is in dat kader van oudsher sprake van een dilemma tussen het verhogen van veiligheid en het inleveren van privacy. Die afweging is uiteindelijk geen wetenschappelijke, maar een politieke keuze. Uit de internationale literatuur blijkt dat te mate van aantasting van privacy per toepassing en per organisatie kan verschillen. Bij predictive policing kan bijvoorbeeld de focus liggen op risicoplekken en risicopersonen. Bij het voorspellen van criminaliteit op 'hotspots' is de aantasting van privacy niet aan de orde, maar bij het voorspellen van criminele gedragingen van personen die op een watch list staan wel. In Nederland ligt de focus op 'places', maar in de Verenigde Staten zijn ook voorbeelden van predictive policing gevonden waar de focus lag op 'persons'. Dit voorbeeld laat zien dat de inzet en focus van specifieke tools per politieorganisatie kan verschillen en daarmee ook de mate waarin specifieke risico's zich kunnen manifesteren. De privacy van burgers kan zichtbaar, maar ook heimelijk worden aangetast. Bij slimme camera's die zichtbaar in de publieke ruimte zijn geplaatst, kunnen burgers weten dat er beelden worden geregistreerd, maar dit is niet het geval bij drones die op afstand beeldmateriaal verzamelen. Bij het gericht volgen van verdachte personen is dat onvermijdelijk en minder bezwaarlijk (omdat hier een motivering en zorgvuldige afweging aan ten grondslag ligt) dan bij het ongericht volgen van onschuldige burgers. Een ander risico is de *kans op fouten*. Hoewel mensen ook fouten kunnen maken, zijn er sterke aanwijzingen dat fouten in systemen minder worden geaccepteerd in de samenleving dan menselijke fouten. Een aannemelijke verklaring is dat bij menselijke fouten ook mensen aansprakelijk kunnen worden gesteld, terwijl dat bij AI-systemen veel lastiger is. Fouten in AI-systemen kunnen bijvoorbeeld worden toegeschreven aan de bouwers van deze systemen, maar ook aan de gebruikers en dat kunnen mensen zijn die de data onjuist interpreteren en op basis daarvan foute of onjuiste interventies plegen. Fouten in AI-systemen kunnen ingrijpende gevolgen hebben voor burgers. Ze kunnen bijvoorbeeld onterecht in risicoprofielen belanden of ten onrechte als verdachte personen worden aangemerkt.

Risico's die in iets mindere mate zijn vermeld in de literatuur hebben betrekking op doelverschuiving, aantasting van discretionaire ruimte, aantasting van de kwaliteit van interacties, dominantie van private bedrijven en militarisering van de politie. *Doelverschuiving* treedt op wanneer data voor andere doeleinden worden gebruikt dan waarvoor ze verzameld zijn. Een voorbeeld is kentekenregistratie door slimme camera's. Het doel daarvan kan zijn om voertuigen te detecteren, maar dit doel kan ook verschuiven naar het detecteren van verdachte personen in deze voertuigen. In dat laatste geval kan de privacy van burgers in het geding zijn. Doorgaans is er een wettelijke basis die de doelbinding bepaalt en dit verkleint de kans op onrechtmatige dataverzameling. Verder kan AI resulteren in een *aantasting van discretionaire ruimte* van professionals binnen de politie. De mate waarin de handelingsruimte van politieprofessionals wordt ingeperkt, kan per toepassing verschillen. In sommige gevallen wordt er veel gewicht toegekend aan het gezonde verstand van professionals bij de politie, terwijl er in andere gevallen (blind) wordt vertrouwd op AI-systemen. Dat verschil werd bijvoorbeeld zichtbaar bij predictive policing, waarbij uit de literatuur bleek dat de ruimte voor het professionele menselijke oordeel per politieorganisatie kan variëren. Het is belangrijk dat er voldoende ruimte is voor het gezond verstand van professionals, om eventuele systeemfouten tijdig te signaleren en te voorkomen. AI kan een negatieve impact hebben op de *kwaliteit van de interacties* tussen de politie en de samenleving. Digitaal contact kan als afstandelijk en minder prettig worden ervaren dan persoonlijk 'warm' contact, maar dat is mede afhankelijk van de specifieke context. Voor standaardaangiften kan digitaal contact een prima alternatief zijn, terwijl er bij ingrijpende gebeurtenissen juist behoefte kan zijn aan persoonlijke contacten met de politie. Het is daarom belangrijk dat de burgers via verschillende communicatiekanalen de politie kunnen benaderen. In de literatuur over (digitale) dienstverlening wordt in dat kader gewezen op het belang van multi

channeling. Burgers zijn immers een belangrijke informatiebron voor de politie. Een ander risico is de *dominantie van private bedrijven.* In de Verenigde Staten wordt bijvoorbeeld veel AI-technologie geleverd door private partijen en dit kan resulteren in een eenzijdige afhankelijkheidsrelatie tussen politieorganisaties en de leveranciers van AI-technologie. In Europa ligt in dit verband het mogelijke risico op de loer dat politieorganisaties afhankelijk kunnen worden van AI-technologie die elders (bijvoorbeeld door Chinese leveranciers) ontwikkeld wordt. Een risico dat specifiek is genoemd bij automated policing in de Verenigde Staten is *militarisering van de politie*. Dit risico werd bijvoorbeeld expliciet in de Amerikaanse literatuur benoemd bij de inzet van een bomrobot door de politie in Dallas. Militarisering kan de afstand tussen burgers en de politie vergroten en in het uiterste geval ervoor zorgen dat burgers en de politie letterlijk lijnrecht tegenover elkaar komen te staan. In andere landen zijn nog geen bomrobots ingezet, maar niemand kan uitsluiten dat dit in de toekomst gebeurt.

Deelvraag 3: Wat zijn de kritische succesfactoren bij de toepassing van AI door de politie?

Uit de internationale literatuur zijn tien kritische succesfactoren afgeleid. Deze factoren zijn bepalend bij het effectief inzetten van AI door de politie (en in de keten betrokken organisaties). De **eerste** kritische succesfactor is *de acceptatie van AI* en andere nieuwe technologieën binnen de politie en de samenleving. Deze factor verwijst naar het draagvlak voor het inzetten van nieuwe technologie. De **tweede** kritische succesfactor betreft *de kwaliteit en de kwantiteit van data*. Hoe meer (hoogwaardige) data de politie bezit, hoe optimaler het leerproces van AI-systemen, omdat de kwaliteit en effectiviteit van dit leerproces immers in belangrijke mate wordt bepaald door de hoeveelheid en de kwaliteit van de data waarover de politie beschikt. Tegelijkertijd kan de politie, afhankelijk van de context, niet ongelimiteerd data verzamelen. In Europa, dus ook in Nederland, zijn de EVRM en de AVG bijvoorbeeld van invloed op de hoeveelheid en aard van de gegevens die de politie mag verzamelen. Een **derde** kritische succesfactor is de *IT-infrastructuur*. De inzet van AI door de politie vereist een interne IT-infrastructuur die daarvoor is toegerust en dus toereikend is om grote hoeveelheid data te verwerken en te analyseren. Een **vierde** kritische succesfactor betreft de *verdere professionalisering* binnen de politie. Het gebruik van AI binnen politieorganisaties vereist ook nieuwe kennis, vaardigheden en competenties van politieprofessionals. Dit betreft onder meer het correct invoeren van data in AI-systemen, het juist interpreteren van data in AI-systemen en het op basis daarvan effectieve interventies te plegen. De vereiste kennis, vaardigheden en competenties moeten tijdens de opleiding of via (bij)scholingstrajecten overgedragen worden aan politieprofessionals. De **vijfde** kritische succesfactor betreft *menselijke oordeelsvorming*. Het is belangrijk dat er binnen politieorganisaties voldoende ruimte is voor het menselijke oordeel als dubbelcheck om fouten en biases te signaleren. Uit de bestudeerde literatuur blijkt dat de ruimte voor het professionele oordeel bij politieorganisaties kan variëren. In sommige gevallen wordt er in belangrijke mate (blind) vertrouwd op de uitkomsten van AI-systemen, terwijl er bij andere cases meer gewicht wordt toegekend aan het 'gezond verstand' van politieprofessionals. De **zesde** kritische succesfactor is *transparantie*. Veel AI-systemen fungeren in zekere mate als 'black box' waardoor uitkomsten voor experts vaak wel, maar voor leken vaak niet (goed) te doorgronden zijn. Dat probleem kan worden vergroot wanneer politieorganisaties bij AI-toepassingen afhankelijk zijn van externe leveranciers. Als de politie op basis van AI specifieke interventies pleegt, dan is het belangrijk dat dit goed kan worden uitgelegd aan de samenleving en de burgers. De **zevende** kritische succesfactor is *wettelijke inkadering*. Discriminatie en de aantasting van de privacy van burgers zijn in de internationale literatuur in dat kader benoemd als de belangrijkste risico's. Daarom is het belangrijk dat er voldoende juridische waarborgen zijn om discriminatie en de onnodige aantasting van privacy van burgers te voorkomen. Vanwege opsporingsbelangen kan de privacy van (verdachte) burgers in het geding zijn. In dat geval is een belangrijke rol als 'waakhond' weggelegd voor toezichthouders. De **achtste** kritische succesfactor is het *periodiek evalueren* van de ervaringen die met AI worden opgedaan. In de literatuur zijn weinig tot geen artikelen gevonden die

inzicht bieden in evaluaties die binnen de politie zijn uitgevoerd. Hiermee is niet gezegd dat er niet wordt geëvalueerd, maar in dat geval worden de lessen in beperkte kring (intern) gedeeld, terwijl bij meer transparantie het leerpotentieel zou kunnen worden verhoogd. Hiermee is niet gezegd dat er tot in detail gerapporteerd moet worden over de bevindingen, omdat een dergelijke transparantie criminelen in de kaart kan spelen. Op basis van de uitgevoerde evaluaties kunnen ook beredeneerde kosten-batenanalyses worden uitgevoerd waarbij de verwachte opbrengsten en vereiste investeringen (hardware en software) tegen elkaar worden afgewogen. De **negende** kritische succesfactor heeft betrekking op *ethische richtlijnen*. In de internationale literatuur is in dat kader gewezen op drie principes, namelijk suitability, necessity & proportionality. Bij iedere AI-toepassing moet dus de vraag worden gesteld of de tool passend, noodzakelijk en proportioneel is. In de Europese Unie zijn de ethische richtlijnen voor betrouwbare kunstmatige intelligentie een belangrijke ethische basis (Europese Commissie, 2019). De EC onderscheidt vier ethische beginselen, namelijk respect voor menselijke autonomie, preventie van schade, rechtvaardigheid en verantwoording. De **tiende** kritische succesfactor is *(digitale) dataveiligheid*. Naarmate de hoeveelheid digitale data die de politie verzamelt en bewerkt toeneemt, neemt ook het belang van dataveiligheid toe. Het is van groot belang dat (privacygevoelige) data binnen politieorganisaties op een veilige manier worden gedeeld en opgeslagen en dat deze (privacygevoelige) data niet in handen komen van hackers of infiltranten.

Deelvraag 4: Welke rol spelen contextuele factoren bij de mogelijke inzet van AI?

In de internationale literatuur wordt er, veelal indirect, aandacht besteed aan contextuele factoren die mede van invloed zijn op de mogelijke inzet van AI. Een organisatorische factor is de mate van centralisatie van de politie. Bij een gecentraliseerd politieapparaat is er meer regie bij de ontwikkeling en toepassing van AI, terwijl bij een gedecentraliseerd politieapparaat organisatieonderdelen meer autonomie hebben. Een culturele factor betreft de politiecultuur. In het ene land is de afstand tussen de politie en burgers groter dan in het andere land. In de Verenigde Staten is die afstand bijvoorbeeld groot. Deze afstand wordt in de Verenigde Staten verder vergroot door de 'militarisering' van de politie waarbij de politie en burgers vaak lijnrecht tegenover elkaar staan. Een maatschappelijke factor dat hiermee samenhangt, is de mate van vertrouwen van burgers in de politie. Er zijn landen waar burgers een groot wantrouwen hebben richting de politie en er zijn landen waar sprake is van (meer) wederzijds vertrouwen tussen politie en burgers. Een juridische factor betreft de wettelijke kaders waarbinnen de politie moet opereren. Deze kaders kunnen per land verschillen. In de Europese Unie zijn het Europees Verdrag voor de Rechten van de Mens (EVRM) en de Algemene verordening gegevensbescherming (AVG) belangrijke kaders om de mensenrechten en privacy van burgers te beschermen. Deze kaders hebben invloed op de toepassingsmogelijkheden van AI door de politie binnen deze landen. In landen als de Verenigde Staten zijn er minder privacywaarborgen, om nog maar te zwijgen over landen als China, waar grote stappen lijken te worden gezet met AI, omdat de privacy van burgers voor de overheid geen belemmering vormt.

De Nederlandse politiecontext

In hoofdstuk 7 is er (globaal) aandacht besteed aan contextuele factoren die van toepassing zijn op de Nederlandse politie. Met deze factoren moet namelijk rekening worden gehouden om de internationale inzichten te 'vertalen' naar conclusies en concrete aandachtspunten voor de (Nederlandse) politie. In dat kader zijn de hoofdbevindingen van deze internationale literatuurstudie ook ter commentaar voorgelegd aan kritische meelezers binnen de Nederlandse politie. Er is bij de contextuele factoren een onderscheid te maken tussen juridische, organisatorische, maatschappelijke en institutionele factoren. Deze factoren zijn van invloed op de (uitvoerings)ruimte om met AI aan de slag te gaan.

Relevante contextuele juridische kaders voor de Nederlandse politie (en andere politieorganisaties in de Europese Unie) zijn het EVRM, de AVG en de Wpg. De Wpg regelt de verwerking van persoonsgegevens voor de uitoefening van de politietaak door onder meer de Nationale Politie, de bijzondere opsporingsdiensten, de Koninklijke marechaussee en de Rijksrecherche. De politie in de Europese Unie, inclusief Nederland, kan dus AI niet ongelimiteerd inzetten en moet de mensenrechten en privacy van burgers in de Europese Unie respecteren.

Een relevante contextuele organisatorische factor voor de Nederlandse politie is de mate van centralisatie. In Nederland is er als gevolg van de reorganisatie tot de Nationale Politie sprake van een hoge mate van centralisatie. Dit betekent in principe dat in Nederland de toepassingen op het AI centraal worden ontwikkeld. Tegelijkertijd is er ook ruimte voor decentrale innovaties bij de politie-eenheden. In de landen zoals de Verenigde Staten ontbreekt centrale regie en hebben politieorganisaties een hoge mate van decentrale autonomie, en kunnen er dus grote verschillen bestaan in de mate waarin en de wijze waarop AI-toepassingen worden geïmplementeerd.

Een relevante contextuele maatschappelijke factor voor de Nederlandse politie is de mate van vertrouwen. In Nederland hebben burgers relatief veel vertrouwen in de politie. In landen als de Verenigde Staten is het vertrouwen van burgers in de politie aanzienlijk lager. De mate van vertrouwen is van invloed op het draagvlak voor innovatie en de ruimte die de politie heeft om AI-toepassingen te implementeren. Het is namelijk cruciaal dat nieuwe toepassingen het vertrouwen van burgers in de politie niet aantasten, omdat dit ten koste gaat van de slagkracht en effectiviteit van de politie. Wanneer burgers minder vertrouwen hebben in de politie, dan zal de bereidheid om aangifte te doen bij de politie of om informeel gegevens te delen met de politie dalen.

Een relevante institutionele factor voor de Nederlandse politie is de inbedding in de veiligheidsketen. In de bestudeerde artikelen is de politie vaak als geïsoleerde casus benaderd, terwijl politieorganisaties wereldwijd een onderdeel zijn van de veiligheidsketen. Het toepassen van AI door een specifieke ketenpartner kan doorwerken in de hele veiligheidsketen. Een concreet voorbeeld is de bewijslast die de politie met AI kan vergaren. De vraag is in hoeverre dit bewijsmateriaal wordt erkend door rechters. Daarom is het belangrijk dat ketenpartners ook anticiperen op innovaties die binnen de veiligheidsketen worden uitgerold en dat de politie de ketenpartners (pro)actief betrekt bij innovaties binnen de eigen organisatie (zie aandachtspunt 5).

Deelvraag 5: Concrete aandachtspunten voor de (Nederlandse) politie

Op basis van deze literatuurstudie kunnen vijf concrete conclusies worden getrokken waaruit vijf concrete aandachtspunten zijn afgeleid.

Eerste conclusie: De impact van AI op het microniveau is onderbelicht.

Het valt op dat in de bestudeerde literatuur aanzienlijk meer aandacht wordt besteed aan de impact van AI op macro- en mesoniveau, terwijl de impact van AI op individuele politieprofessionals en individuele burgers in veel mindere mate wordt belicht, terwijl uiteindelijk individuele ervaringen bepalend zijn voor het draagvlak voor AI. Zowel politieprofessionals als burgers zullen uiteindelijk ontvankelijk moeten zijn voor specifieke toepassingen. Daarom is het belangrijk om bij de ontwikkelfase en implementatie van nieuwe technologie ook de ervaringen van individuele politieprofessionals en burgers in kaart te brengen. Een concreet aandachtspunt is dat de focus in de internationale literatuur (en dus ook van politieonderzoekers en politieorganisaties) moet worden verlegd naar individuele stakeholders op wie de technologie impact heeft, dus specifiek burgers en politiemedewerkers. Die impact is mede afhankelijk van de context en de specifieke AI-toepassing. Het is verder van groot belang dat de techniek (AI) in balans is met menselijke kennis en verwachtingen.

De professionaliteit van politiemensen moet niet worden onderschat. Vanuit deze overweging vervangt AI de politieprofessionals niet, maar ondersteunt hen op basis van complementariteit.

Tweede conclusie: Veel beschouwend onderzoek, weinig empirisch onderzoek.

Op basis van de bestudeerde internationale literatuur is geconcludeerd dat het aantal empirisch gefundeerde artikelen schaars is. Datzelfde geldt voor de mate waarin onafhankelijke externe evaluaties naar concrete AI-toepassingen door de politie worden belicht in de internationale literatuur. Er wordt door politieorganisaties in binnen- en buitenland volop geëxperimenteerd met nieuwe toepassingen in de vorm van pilots, maar, afgaand op de bestudeerde literatuur, wordt er over de resultaten van de evaluaties niet of nauwelijks gepubliceerd. Voor zover het niet botst met operationele belangen, is het van groot belang dat de ervaringen worden gepubliceerd. Dit helpt politieorganisaties bij het opstellen van een beredeneerde implementatiestrategie. Empirisch onderzoek kan ook behulpzaam zijn bij het maken van zorgvuldige en evidence-based afwegingen met betrekking tot de mate waarin, en de wijze waarop AI wordt ingezet. Ook empirisch gefundeerde ervaringen die buiten de politie met AI worden opgedaan, kunnen waardevol zijn voor politieorganisaties. Actoren moeten daarbij niet zelf het wiel uitvinden, maar ook leren van elkaars ervaringen en activiteiten op elkaar afstemmen.

Derde conclusie: Veel ethische vragen, weinig maatschappelijk debat.

Uit de internationale literatuurstudie blijkt dat AI de nodige ethische vragen oproept. Daarom is het belangrijk dat AI op een beredeneerde, transparante en verantwoorde manier wordt ingezet en dat er sprake is van toezicht en controle. Dit kan in de vorm van audits en periodieke evaluaties. In de internationale literatuur wordt systematisch gepleit voor een debat over AI en het opstellen van kaders, waarbij ethische en juridische aspecten belangrijke aandachtspunten zijn. Zowel het debat als het bepalen van de kaders moeten voortdurend worden gevoerd. Deze discussie is noodzakelijk om de ethische grenzen bij de toepassing van AI te bepalen. Dit debat is breder dan de toepassing van AI op het veiligheidsdomein, maar omvat ook de toepassing van AI op andere domeinen, bijvoorbeeld binnen het ‘smart city’ concept. Een debat kan ook behulpzaam zijn om het maatschappelijk draagvlak voor AI inzichtelijk te maken en bezwaren van burgers voor het voetlicht te brengen.

Vierde conclusie: Interne bedrijfsvoering onderbelicht.

Zoals eerder aangegeven, is er weinig tot geen internationaal onderzoek uitgevoerd naar de impact van AI op microniveau. Dit betreft onder andere de impact op de benodigde competenties, kennis en digitale vaardigheden van politieprofessionals, het vraagstuk van de opleiding, werving en professionalisering van politiemedewerkers, de arbeidssatisfactie van medewerkers, de benodigde IT-infrastructuur en informatiemanagement. Deze les is conform een literatuurstudie die eerder werd uitgevoerd (De Kool, Vermeeren & Steijn, 2020). In het betreffende onderzoek werd gepleit om bij het meten van de impact van AI, de focus te verbreden naar de interne bedrijfsvoering (PIOFACH) en AI niet louter te benaderen als technologische uitdaging, maar ook als een menselijke en organisatorische verandermanagementopgave.

Vijfde conclusie: Weinig onderzoek naar impact van AI op (bredere) veiligheidsketen.

In de bestudeerde literatuur zijn AI-toepassingen belicht die binnen de politieorganisaties zijn of worden uitgevoerd. Daarbij is er nauwelijks aandacht voor de bredere impact in de veiligheidsketen. In een eerder onderzoek hebben wij in dat kader gewezen op de impact van een slimmer en effectiever aangifteproces op het OM (De Kool, Vermeeren & Steijn, 2020). Immers, hoe beter en completer de aangiftedossiers zijn, hoe groter de kans dat het OM effectief met deze dossiers aan de slag kan. Dit

betekent dat de politie en het OM ook voldoende capaciteit moeten hebben om meer dossiers af te handelen. Eenzelfde redenering kan worden opgezet voor de AI-toepassingen die in deze internationale literatuurstudie zijn belicht. AI-toepassingen die door de politie effectief worden ingezet, kunnen de werklast van ketenpartners (OM, CJIB en FIOD bijvoorbeeld) verhogen. De politie moet AI niet alleen benaderen vanuit het eigen organisatieperspectief, maar het bredere technologische ecosysteem in ogenschouw nemen. Dit impliceert dat ook verkokering binnen organisaties en tussen organisaties op het veiligheidsdomein wordt doorbroken, en actoren binnen en buiten het veiligheidsdomein intensiever met elkaar samenwerken, digitale data delen (binnen de geldende juridische kaders) en gezamenlijk innoveren. Ketensamenwerking met andere actoren is noodzakelijk om criminaliteit effectief aan te pakken. Dat geldt dus ook bij het ontwikkelen en implementeren van AI-technologie in de veiligheidsketen.

Hoofdstuk 1: Inleiding

1.1 Aanleiding en probleemstelling

De technologische ontwikkelingen in de samenleving gaan razendsnel. Nieuwe technologieën, zoals Artificiële Intelligentie (hierna te noemen: AI), hebben een steeds grotere invloed op de manier waarop wij leven en werken. AI wordt beschouwd als één van de belangrijkste strategische technologieën van deze eeuw (Europese Commissie, 2018) en één van de sleuteltechnologieën in de digitale transitie (Bakker e.a., 2021).

Tegen deze achtergrond is in Nederland het Strategische Actieplan voor AI gelanceerd.[1] Het belang van AI wordt ook binnen de politieorganisatie onderkend, die als partner is aangehaakt bij het genoemde actieplan. Deze ontwikkeling is een belangrijke aanleiding geweest om een internationale literatuurstudie uit te voeren op het gebied van AI bij de politie.

Deze internationale literatuurstudie bouwt voort op het onderzoeksrapport 'kunstmatige intelligentie bij de politie: praktische en sociale lessen ten aanzien van het aangifteproces' dat werd uitgevoerd in opdracht van het nationaal politielab AI (De Kool, Vermeeren & Steijn, 2020). In dit verkennende onderzoek stond de verwachte sociale impact van AI ten aanzien van het aangifteproces centraal.

AI is een breed en diffuus begrip. In de literatuur is er (nog) geen eenduidige en gezaghebbende definitie van AI. Iedere definitie roept discussie op. In deze literatuurstudie wordt de volgende werkdefinitie van kunstmatige intelligentie gehanteerd: "artificial intelligence refers to systems that display intelligent behavior by analyzing their environment and taking actions – with some degree of autonomy – to achieve specific goals" (High Level Expert Group on Artificial Intelligence - HLEG). De AI HLEG adviseert de Europese Commissie bij het opstellen van nieuwe wetgeving en nieuw beleid op het gebied van AI. Daarmee is deze definitie gangbaar in Europa.

In deze internationale literatuurstudie worden de (empirische) ervaringen van de politie in het buitenland met AI zoals deze zijn beschreven in de internationale wetenschappelijke literatuur weergegeven. Er is dus geen veldwerk ter plekke uitgevoerd. Een gedeelde noemer is dat de inzet van AI door de politie geen doel op zichzelf is, maar een middel om het overkoepelende doel van het veiligheidsdomein te bereiken, namelijk het veiliger maken van de samenleving (De Kool, Vermeeren & Steijn, 2020).

De verwachtingen van AI-toepassingen zijn groot. De politie verwacht dat AI de slagkracht en efficiency van de organisatie aanzienlijk vergroot.[2] Desondanks is het ook van groot belang om AI-toepassingen kritisch te benaderen en om ook oog te hebben voor (vermeende) risico's en de noodzakelijke randvoorwaarden om AI effectief en efficiënt in te zetten. Deze literatuurstudie beoogt inzicht te verschaffen in de resultaten die de politie elders met AI heeft geboekt, de daadwerkelijke risico's van en de noodzakelijke kritische succesfactoren die ervoor zorgen dat AI effectief en succesvol kan worden ingezet.

Om de juiste lessen te kunnen trekken uit de ervaringen die elders worden opgedaan, is het van groot belang om rekening te houden met de specifieke context waarin de politie in verschillende landen opereert. De context kan verschillen per land, maar zelfs binnen een land. Op macroniveau kan een

[1] https://www.rijksoverheid.nl/documenten/beleidsnotas/2019/10/08/strategisch-actieplan-voor-artificiele-intelligentie

[2] https://www.politie.nl/nieuws/2019/januari/16/%E2%80%98kunstmatige-intelligentie-vergroot-onze-slagkracht.html

onderscheid worden gemaakt tussen de wijze waarop de Verenigde Staten, China en de Europese Unie omgaan met AI. In de Verenigde Staten is een belangrijke rol weggelegd voor het bedrijfsleven, terwijl in China de overheid de regie strak in handen heeft en privacy van burgers eigenlijk geen aandachtspunt is. China loopt momenteel weliswaar voorop met de ontwikkeling van AI, maar een belangrijke kanttekening daarbij is dat in China niet of nauwelijks rekening wordt gehouden met de privacy van burgers.[3] Om die reden valt casuïstiek bij de Chinese politie buiten de focus van deze literatuurstudie.

In de Europese Unie wordt wel veel belang gehecht aan de bescherming van de privacy van burgers. In de Europese Unie zijn het Europees Verdrag voor de Rechten van de Mens (EVRM) en de Algemene Verordening Gegevensbescherming (AVG) belangrijke kaders. De AVG beoogt de privacy van burgers in de Europese Unie te beschermen. Dit kader is ook van invloed op de ambities van de Europese Unie op het gebied van AI. De Europese Commissie heeft de doelstelling op het gebied van AI als volgt geformuleerd: "the objective of the Union being a global leader in the development of secure, trustworthy and ethical artificial intelligence." (European Commission, 2021a). In een ander document is de Europese ambitie als volgt omschreven: "to become the world-leading region for developing and deploying cutting-edge, ethical land secure, AI, (and) promoting a human-centric approach in the global context (European Commission, 2021b, p. 56). Het realiseren van deze ambitie vereist grote investeringen: "the Commission proposed that the Union invest in AI at least EUR 1 billion per year (…) under the programming period 2021-2027" (European Commission, 2021b).

Uit deze passages blijkt dat de ambities van de Europese Unie op het gebied van AI groot zijn, maar dat tegelijkertijd wordt ingezet op een ethisch verantwoorde inzet van AI en dat van een ongereguleerde opmars van AI in de Europese Unie geen sprake kan zijn. In de Europese Unie wordt veel belang gehecht aan Europese waarden, fundamentele rechten en principes. De toepassing van AI moet daarmee in overeenstemming zijn. De Europese Commissie heeft op 21 april 2021 strenge concept wetgeving en voorgenomen acties gepubliceerd over de toepassing van kunstmatige intelligentie. De internationale (en nationale) kaders waarbinnen politieorganisaties opereren zijn dus belangrijke contextuele factoren om rekening met te houden.

Om de kansen en risico's van AI, evenals de noodzakelijke randvoorwaarden en concrete aandachtspunten voor de (Nederlandse) politie goed voor het voetlicht te krijgen, is het van groot belang dat er niet louter wordt gekeken naar de ontwikkelingen op het gebied van AI die zich in Nederland voltrekken, maar dat ook de ontwikkelingen en ervaringen op het gebied van AI bij politieorganisaties in het buitenland systematisch in kaart worden gebracht, zodat de politie daar inspiratie uit kan putten en het wiel niet opnieuw hoeft uit te vinden.

Politieorganisaties experimenteren wereldwijd volop met de mogelijkheden van AI. In ons eerdere onderzoeksrapport werd de aanbeveling gedaan om de ontwikkelingen op het gebied van AI bij politieorganisaties in het buitenland nader in kaart te brengen (De Kool, Vermeeren & Steijn, 2020). Een kanttekening is wel dat de adoptie van AI-systemen bij veel politieorganisaties zich nog in een vroege (pioniers)fase lijkt te bevinden: "The adoption of AI systems in policing is still in its early stages" (Joh, 2018a). We zijn nu enkele jaren verder, dus mogelijk zijn de ervaringen met AI inmiddels beter geborgd en ingedaald in politieorganisaties. De beoogde literatuurstudie zal dit nader moeten uitwijzen. Dit brengt ons bij de doelstelling van het onderzoek.

[3] https://www.nu.nl/tech/6161668/ex-softwarechef-luchtmacht-vs-ai-achterstand-op-china-niet-meer-in-te-halen.html

1.2 Doelstelling van het onderzoek

De doelstelling van dit onderzoek is om op basis van beschikbare internationale literatuur (empirische) inzichten te vergaren in de ervaringen die politieorganisaties in het buitenland opdoen met kunstmatige intelligentie en op basis daarvan concrete conclusies en aandachtspunten te formuleren voor de (Nederlandse) politie. In het bijzonder is daarbij aandacht besteed aan kansen, risico's en kritische succesfactoren voor de samenleving (macroniveau), de politieorganisatie (mesoniveau) en individuele burgers en politieprofessionals (microniveau). De ervaringen die de politie elders opdoet met AI kan de Nederlandse politie behulpzaam zijn bij het beredeneerd en effectief implementeren van AI-toepassingen.

Hierbij dient te worden opgemerkt dat positieve of negatieve ervaringen die de politie in het buitenland opdoet dan wel heeft opgedaan met AI, niet per definitie relevant of bruikbaar zijn voor de Nederlandse politiepraktijk. In de vorige paragraaf is vastgesteld dat de context waarbinnen de politie opereert en functioneert variëren. In dat kader kan een onderscheid worden gemaakt tussen de interne context (bijvoorbeeld de specifieke politiecultuur), de maatschappelijke context, de politiek-bestuurlijke context, de juridische context en de bredere context van de veiligheidsketen.

Deze doelstelling maakt duidelijk dat er bij dit onderzoek geen veldwerk ter plekke wordt uitgevoerd en dat relevante casuïstiek bij de politie in het buitenland waarover (nog) niet is gepubliceerd, buiten de focus van dit onderzoek vallen. Een ander relevant aandachtspunt is dat dit onderzoek de semantische discussie over wat wel en niet AI is niet beoogt te beslechten. Op voorhand mag bij een brede internationale literatuurstudie ervan worden uitgegaan dat de auteurs AI op uiteenlopende manieren zullen benaderen en definiëren.

Daarom wordt AI in dit onderzoek niet benaderd als een dichotomie (wel/niet AI), maar als een innovatie waarbij de mate van intelligentie kan variëren. Dit is in lijn met het onderzoek van De Kool, Vermeeren en Steijn (2020) waarbij drie verschillende vormen of niveaus zijn onderscheiden, namelijk taakspecifieke AI, brede AI en superintelligentie. De mate van AI kan dus per toepassing variëren. De verwachting is dat de toepassingen met taakspecifieke AI het meest gangbaar zijn bij de politie in het buitenland, de toepassingen op het gebied van brede AI nog beperkt zijn en dat toepassingen op het gebied van superintelligentie nog niet aan de orde zijn en nog toekomstmuziek zijn. De beoogde literatuurstudie zal uitwijzen of en in hoeverre dit het geval is.

In het reeds genoemde onderzoek van De Kool, Vermeeren en Steijn (2020) is de inzet van AI niet primair benaderd als een technologische innovatie, maar als een sociale en organisatorische veranderingsopgave. AI heeft daarbij niet alleen impact op het primaire proces, maar ook op ondersteunde processen. In het onderzoek bleken de respondenten een duidelijke behoefte te hebben om de blik naar buiten te richten en kennis te nemen van ervaringen die elders zijn en worden opgedaan met AI. Dit kunnen positieve en negatieve lessen zijn, maar ook onbedoelde en onvoorziene gevolgen die AI kan hebben binnen de politie (en veiligheidsketen).

Bepaalde ervaringen kunnen mogelijk fungeren als inspiratiebron of wenkend perspectief, maar er kunnen ook ervaringen boven tafel komen, waarbij het voor de Nederlandse politie niet haalbaar of wenselijk is om bepaalde wegen met AI in te slaan, bijvoorbeeld omdat deze de cruciale 'verbinding' tussen de politie en burgers aantasten. De inzet van AI in het aangifteproces kan bijvoorbeeld alleen effectief zijn, wanneer de aangiftebereid van burgers op peil blijft of verder wordt vergroot.

De ervaringen elders helpen de politie in Nederland bij het maken van beredeneerde keuzes om AI op bepaalde gebieden wel, en op andere gebieden niet of in mindere mate in te zetten. Het is en blijft

namelijk van groot belang om kritisch te blijven nadenken over de vraag hoe de politie AI als middel effectief en zinvol kan inzetten om haar maatschappelijke doelen te bereiken en de Nederlandse samenleving veiliger te maken. Ook (vermeende) successen in het buitenland dienen op een nuchtere en kritische manier te worden benaderd.

1.3 Onderzoeksvragen

De probleemstelling resulteert in de volgende centrale vraagstelling: *Welke empirisch gefundeerde lessen kunnen worden getrokken uit de in de internationale literatuur belichte ervaringen die politieorganisaties in het buitenland opdoen of hebben opgedaan met de beoogde en gerealiseerde implementatie van concrete AI-toepassingen, en welke casuïstiek en concrete aandachtspunten kunnen op basis van deze internationale ervaringen worden aangereikt op basis waarvan de politie in Nederland AI effectief kan inzetten om haar doelen te bereiken?*

Deze vraagstelling valt uiteen in de volgende vijf deelvragen:

1. Welke (verwachte) kansen van AI worden in de internationale politieliteratuur waargenomen?
2. Welke (verwachte) risico's van AI worden in de internationale politieliteratuur waargenomen?
3. Welke kritische succesfactoren kunnen uit de vergelijking van de cases in de deskstudie worden gedestilleerd om AI effectief en succesvol in te zetten?
4. Welke rol speelt de interne context (politiecultuur), de maatschappelijke context, de politiek-bestuurlijke context, de juridische context en de bredere context van de veiligheidsketen bij de mogelijke inzet van AI?
5. Hoe kunnen de vergaarde empirische inzichten uit de internationale politieliteratuur in samenwerking met de Nederlandse politie worden vertaald naar concrete, beredeneerde en bruikbare aandachtspunten voor de (Nederlandse) politiepraktijk?

1.4 Leeswijzer

In hoofdstuk 2 worden de onderzoeksopzet en gehanteerde onderzoeksmethoden verantwoord. De resultaten van de internationale literatuurstudie zijn beschreven en geordend op basis van drie dominante thema's die in de literatuur naar voren zijn gekomen. Deze thematische indeling is dus niet vooraf bedacht, maar vloeit voort uit de resultaten van het onderzoek. In hoofdstuk 3 wordt het thema predictive policing belicht. In hoofdstuk 4 wordt aandacht besteed aan het thema smart policing. In hoofdstuk 5 staat het thema automated policing centraal. In hoofdstuk 6 worden de overige slimme toepassingen in kaart gebracht. In hoofdstuk 7 worden de resultaten van de gesprekronde met politieonderzoekers, de onlinefocusgroep en activiteiten op het gebied van AI binnen de Nederlandse politiecontext belicht. In hoofdstuk 8 staan de conclusies en aandachtspunten.

Hoofdstuk 2: Methodologische verantwoording

Deze internationale literatuurstudie is gericht op het analyseren en bestuderen van Engelstalige wetenschappelijke literatuur over de toepassing van AI door de politie in het buitenland. Dit impliceert dat geen veldonderzoek is uitgevoerd en casuïstiek waarover (nog) niet is gepubliceerd, niet is meegenomen in de analyse. De beoogde analyse omvat drie niveaus, namelijk het macroniveau, het mesoniveau en het microniveau. De literatuur is geordend en geclusterd op basis van dominante thema's in de literatuur.

Aan de beoogde aanpak en focus op buitenlandse casuïstiek liggen verschillende overwegingen ten grondslag. De eerste overweging is dat de verschillende contexten waarin AI wordt ingezet, de inzichten kan verrijken. Van organisaties die zaken op een heel andere manier benaderen, kan vaak meer worden geleerd dan organisaties die de zaken op dezelfde en dus voorspelbare manier aanpakken. Een les kan zijn om AI op een vergelijkbare manier in te zetten, maar een les kan ook zijn om beredeneerd af te zien van een specifieke toepassing omdat er veel bezwaren aan kleven.

Een andere overweging is dat de Nederlandse politie op een onbevangen manier kennis kan nemen van de ervaringen die in het buitenland zijn opgedaan. Bij een focus op Nederlandse casussen zou er naar verwachting sprake zijn geweest van minder onbevangenheid, omdat de politie immers stakeholder in het geheel is. Daarom zal de organisatie veel ontvankelijker zijn om lessen te trekken uit ervaringen die elders zijn opgedaan.

Een praktische overweging betreft het feit dat de belasting van de Nederlandse politie bij een buitenlandse deskstudie relatief beperkt is. De werkdruk bij de Nederlandse politie is hoog en daarom is het wenselijk om de Nederlandse politie niet overmatig te belasten met onderzoeksprojecten. De belasting van de politieprofessionals is bij dit onderzoek minimaal omdat primair beschikbare literatuur wordt bestudeerd.

Op voorhand kan een onderscheid worden gemaakt tussen beschouwende literatuur en empirisch gefundeerde literatuur. Bij aanvang van het onderzoek kon nog niet worden overzien of de beschikbare literatuur beschouwend of empirisch van aard was. Bij deze internationale literatuur zijn empirisch gefundeerde artikelen het meest waardevol, omdat deze zijn gebaseerd op reeds opgedane ervaringen bij de politie in het buitenland. Beschouwende artikelen zijn zeker bruikbaar, maar iets minder relevant, omdat daarin doorgaans potentiële kansen en risico's van AI centraal staan en er vaak nog geen inzicht is in de mate waarin deze kansen en risico's zich in de politiepraktijk manifesteren.

Dit onderzoek heeft een gefaseerd karakter, waarbij vier fasen kunnen worden onderscheiden. Het zwaartepunt van het onderzoek is, zoals gezegd, een systematische internationale literatuurstudie, waarbij systematisch is gekeken naar de concrete ervaringen die politieorganisaties in het buitenland opdoen dan wel hebben opgedaan met concrete AI-toepassingen (fase 1). In fase 2 zijn internationale (politie)onderzoekers digitaal geconsulteerd. Zij hebben hun licht laten schijnen op hun publicaties, relevante ontwikkelingen belicht en hun onderzoeksbevindingen in de juiste context geplaatst. Bij empirische en beschouwende observaties moet namelijk rekening worden gehouden met de specifieke context waarin AI-toepassingen zijn of worden geïmplementeerd. In fase 3 zijn de inzichten uit de internationale literatuur digitaal teruggekoppeld in een focusgroep aan politieprofessionals in Nederland met als doel om te verkennen welke concrete en beredeneerde handelingsperspectieven kunnen worden geformuleerd waarbij rekening is gehouden met de Nederlandse context. Dat laatste kwam iets minder goed uit de verf omdat de discussie tijdens de focusgroep werd gedomineerd door een semantische discussie over wat nu wel en niet AI is. Een bijkomende factor was dat het aantal

empirisch gefundeerde artikelen beperkter was dan verwacht. In fase 4 zijn de belangrijkste bevindingen van het onderzoek (samenvatting) ter commentaar voorgelegd aan enkele kritische meelezers binnen de Nederlandse politie. Daarnaast zijn de bevindingen periodiek te commentaar voorgelegd aan en besproken met de begeleidingscommissie (zie bijlage 3). De vier onderscheiden fasen zijn weergegeven in tabel 1.

Tabel 1: Doorlopen onderzoeksfasen en bijbehorende activiteiten.

Onderzoeksfase	**Activiteiten**
Fase 1	Systematische internationale deskstudie van politieliteratuur.
Fase 2	Digitale/telefonische consultatie van buitenlandse politie-experts en verslaglegging.
Fase 3	Digitale focusgroep voor (politie)professionals en verslaglegging.
Fase 4	Belangrijkste bevindingen ter commentaar voorgelegd aan kritische meelezers binnen de politie.

Werkwijze internationale literatuurstudie

Bij de internationale literatuurstudie is getracht om concrete empirische ervaringen met de toepassing van AI die bij politieorganisaties in het buitenland zijn en worden opgedaan, systematisch in kaart te brengen. Daarbij is de volgende aanpak gehanteerd. Het belangrijkste digitale portaal om wetenschappelijke literatuur te verzamelen was Google Scholar. De zoekperiode is afgebakend tot de afgelopen tien jaar, mede omdat de ontwikkelingen op het gebied van AI momenteel snel gaan. Artikelen die voor 2011 zijn verschenen zijn daarom niet bestudeerd. Het zwaartepunt van de bestudeerde literatuur omvat artikelen die zijn gepubliceerd in Engelstalige wetenschappelijke tijdschriften. Er zijn ook hoofdstukken in recente boeken bestudeerd. De meeste artikelen waren beschikbaar. Artikelen achter betaalmuren van uitgevers zijn niet bestudeerd. Om ook de meest recente empirische inzichten mee te kunnen nemen, zijn ook 'online before print' artikelen bestudeerd.

Om relevante artikelen te vinden, zijn de volgende losse zoektermen gehanteerd: predictive policing, prescriptive policing, automated policing, smart policing, smart surveillance, smart sensing, smart sensoring, smart law enforcement, automated law enforcement (systems), smart surveillance, (smart) facial recognition, facial-recognition technology, cybercrime, cybersecurity, (automated) facial recognition technology (FRT), FRT surveillance, automated policing, robotic policing, police robots, data-driven policing.

Daarnaast zijn gecombineerde zoektermen gehanteerd (met combi: 'and/or police'): artificial intelligence, algorithms, patterns, (big) data, robotics, machine learning, data mining, social media monitoring, chatbots, algorithms, (social) innovation, human rights, legitimacy, legality, (public) trust, privacy, transparency, empathy, public values, accountability, human autonomy.

Bij de selectie van de relevante literatuur is tevens de 'sneeuwbalmethode' toegepast, waarbij op basis van de geïnventariseerde literatuur is gekeken naar welke wetenschappelijke publicaties (artikelen en beoeken) wordt doorverwezen en welke trefwoorden in de bestudeerde literatuur zijn vermeld.

In totaal zijn er ruim 175 publicaties bestudeerd die allemaal opgenomen zijn in de literatuurlijst. Bij de bestudeerde literatuur kan een onderscheid worden gemaakt tussen empirisch gefundeerde en beschouwende artikelen. Bij deze deskstudie zijn empirische artikelen het meest relevant omdat deze

inzicht bieden in de empirische ervaringen die politieorganisaties reeds hebben opgedaan. In de hoofdstukken zal blijken dat het aantal empirisch gefundeerde artikelen beperkt is in relatie tot beschouwende publicaties.

De bevindingen zijn geclusterd in drie hoofdstukken op basis van drie thematische begrippen die in de bestudeerde internationale literatuur het vaakst zijn genoemd, namelijk predictive policing, smart policing en automated policing. Bij brede en abstracte concepten is iedere indeling arbitrair. Daar komt bij dat deze drie clusters elkaar niet uitsluiten. Toepassingen die minder goed te plaatsen waren binnen één van de genoemde clusters zijn in een separaat hoofdstuk beschreven en belicht onder het kopje 'overige toepassingen'. De geïnventariseerde casuïstiek is per hoofdstuk geordend en beschreven aan de hand van de volgende aspecten: de gehanteerde werkdefinitie van het betreffende thema, de concrete toepassingen op het betreffende thema, de (beoogde) kansen, de (mogelijke) risico's en kritische succesfactoren.

Binnen de genoemde thema's zijn steeds drie analyseniveaus onderscheiden, namelijk macroniveau (samenleving), mesoniveau (politieorganisatie) en microniveau (individuele politieprofessionals en burgers). Tevens zijn de gesignaleerde ontwikkelingen bij de bestudeerde buitenlandse cases voor zover dat mogelijk was gekoppeld aan vier relevante contexten, namelijk (1) de interne context (de politiecultuur), (2) de maatschappelijke context waarbinnen de politie opereert, (3) de politiek-bestuurlijke context waarbinnen de politie wordt aangestuurd en de (4) bredere context van de veiligheidsketen waarin de politie is ingebed.

Buitenlandse praktijken die te ver afstaan van de praktijken in de Nederlandse democratische rechtstaat zijn in dit onderzoek bewust buiten beschouwing gelaten, omdat de politie in Nederland hier weinig tot geen lessen uit kan trekken. In landen met dictatoriale regimes kan AI bijvoorbeeld door de politie worden gebruikt om burgers te onderdrukken. Dergelijke contexten bieden geen wenkende perspectieven en zijn dus niet bestudeerd.

Hoofdstuk 3: Predictive policing

3.1 Inleiding

Smit e.a. (2016) constateren dat predictive policing een relatief nieuw concept in de wetenschappelijke literatuur is. Ze hebben gelijk voor wat betreft dit Engelstalige begrip, maar wanneer nader wordt ingezoomd op politiepraktijken dan bestaat er bij de politie in binnen- en buitenland een lange traditie om op basis van preventieve maatregelen te proberen om criminaliteit te voorkomen (Perry e.a., 2013). Voorkomen is namelijk beter dan genezen. Een verschil is wel dat de politie met behulp van AI een extra instrument in handen heeft om (mogelijke) criminele gedragingen te voorspellen en wellicht te voorkomen.

In dit hoofdstuk worden de internationale ervaringen van de politie met predictive policing belicht. Een belangrijk uitgangspunt in deze literatuurstudie is dat AI niet wordt benaderd als een dichotomie (wel of geen AI), maar als een breed spectrum waarbij de mate van AI per concrete toepassing kan variëren. Wanneer dit uitgangspunt wordt doorgetrokken naar predictive policing, dan kan de effectiviteit van predictive policing variëren. In de literatuur is gesignaleerd dat de positieve effecten van predictive policing vaak worden overschat (Degeling & Berendt, 2018). De effectiviteit van predictive policing is van verschillende factoren afhankelijk, waaronder de kwaliteit en kwantiteit van de data die fungeren als input voor predictive policing.

In paragraaf 3.2 wordt het begrip predictive policing nader gedefinieerd. In paragraaf 3.3 worden concrete toepassingen van predictive policing in het buitenland beschreven. In paragraaf 3.4 wordt aandacht besteed aan de beoogde kansen van predictive policing en in paragraaf 3.5 worden de mogelijke risico's belicht. In paragraaf 3.6 worden de geïnventariseerde kritische succesfactoren van predictive policing voor het voetlicht gebracht. In paragraaf 3.7 staan de conclusies en reflecties.

3.2 Predictive policing

Predictive policing komt er in het kort op neer dat de politie met behulp van slimme software historische data analyseert met als doel om mogelijke criminele gedragingen in de toekomst te voorspellen en daar tijdig op te anticiperen zodat criminele gedragingen voorkomen kunnen worden.

In de wetenschappelijke literatuur ontbreekt het vooralsnog aan een eenduidige en gezaghebbende definitie van predictive policing (Meijer & Wessels, 2019). Het begrip predictive policing is dus lastig te omschrijven (Spithoven & Beerends, 2019). Wel bestaat er enige consensus over de belangrijkste kenmerken van predictive policing (Meijer & Wessels, 2019).

Het eerste kenmerk is dat predictive policing gebaseerd is op veel en gevarieerde data (Meijer & Wessels, 2019). Dit kunnen bijvoorbeeld potentiële daderprofielen zijn, maar ook geografische data die inzicht bieden in potentiële risicogebieden ('hotspots') waar criminele gedragingen zich kunnen voordoen. In dat kader kan een onderscheid worden gemaakt tussen 'persons' en 'places' (Joh, 2018b; Sandhu & Fussey, 2021). Hung en Yen onderscheiden naast 'persons' en 'places' nog een derde focuspunt, namelijk 'event-based policing' waarbij de focus ligt op het voorspellen van (criminele) activiteiten die met een hoge mate van waarschijnlijkheid gaan plaatsvinden (Hung & Yen, 2021). Van de drie genoemde toepassingsdomeinen is 'person-based' predictive policing het meest controversieel. De focus op places, ofwel de geografische component van predictive policing, is geïntegreerd in de volgende definitie van Egbert (2019): "the application of data analysis technologies by the police to generate and effectuate actionable forecasts of sources and spatiotemporal conditions

of future crime." In deze definitie wordt de nadruk gelegd op (slimme) data-analysetechnologieën om toekomstige criminaliteit te voorspellen.

Het tweede kenmerk van predictive policing is dat de politie op basis van deze analyses preventieve interventies pleegt, dus activiteiten ontplooit voordat criminele handelingen worden verricht in een poging om criminaliteit te voorkomen (Meijer & Wessels, 2019).

Saunders e.a. (2016) maken in hun definitie van predictive policing een expliciet onderscheid tussen een voorspellende analyse en een daarop gebaseerde preventie- of interventiestrategie. Zij constateren: "predictive policing is typically comprised of two elements: a prediction model that uses an algorithm to identify instances of increased crime risk, and an associated prevention strategy to mitigate and/or reduce those risks" (p. 348). Hun benadering omvat dus niet alleen een 'voorspellingsmodel', maar ook een 'preventiestrategie' om criminaliteit te vermijden of te verkleinen ('prevention strategy').

Meijer & Wessels (2019) hanteren een vergelijkbare definitie. Zij definiëren predictive policing als "the collection and analysis of data about previous crimes for identification and statistical prediction of individuals or geospatial areas with an increased probability of criminal activity to help developing policing intervention and prevention strategies and tactics" (p. 1033).

Bennett Moses & Chan (2018) onderscheiden vier fasen bij predictive policing, namelijk data verzamelen, data analyseren, politieoperaties (in hotspots) en de reacties van potentiële criminelen (in de zin dat ze afzien van criminele activiteiten). Zij knippen de twee benoemde kenmerken op in twee specifieke deelactiviteiten.

Op basis van de genoemde omschrijvingen wordt predictive policing in dit onderzoek gedefinieerd als het met behulp van algoritmen analyseren van omvangrijke hoeveelheden geografische data en/of persoonsdata om risico's ten aanzien van mogelijke criminaliteit vroegtijdig in kaart te brengen, en op basis van deze informatie interventies te plegen om daarmee criminele gedragingen te voorkomen of de kans daarop te verkleinen.

In de literatuur zijn we ook een aantal keer de term prescriptive policing tegengekomen. Prescriptive policing voorspelt op basis van de kennis van de effecten van bepaalde interventies wat de effectiviteit van een bepaalde inzet van politiemiddelen zal zijn, gegeven een specifieke situatie (Smit e.a., 2016). Het systeem suggereert dan wat de beste interventie is op basis van een vergelijkbare context, maar uiteindelijk beslissen mensen over de uiteindelijke interventie. Prescriptive policing gaat dus een stapje verder, omdat het nadenken over de beste interventiestrategie ook uit handen genomen wordt.

3.3 Concrete toepassingen in het buitenland

Predictive policing heeft vooral een vlucht genomen in de Verenigde Staten. Veel toepassingen die in deze paragraaf worden belicht hebben dus een Amerikaanse context.

Predictive policing in Philadelphia

Haberman & Ratcliffe (2012) hebben onderzoek gedaan naar predictive policing van de Philadelphia Police Department (PPD). De focus van de PPD lag op het identificeren van hotspots waar (herhaalde) gewapende straatroven plaatsvonden. De onderzoekers concludeerden dat op basis van predictive policing relevante patronen op het gebied van straatroven konden worden geïdentificeerd (bijvoorbeeld ten aanzien van de reeksen), maar dat er nog analytische en organisatorische uitdagingen overwonnen moesten worden om de opgedane inzichten effectief te kunnen toepassen

en vertalen naar specifieke interventies. Er werden drie verschillende interventiestrategieën uitgevoerd en getest, namelijk 'foot patrol', 'problem-oriented policing' en 'offender-focused policing' (Ratcliffe e.a., 2013). Bij foot patrol kregen de politiemensen geen specifieke orders of instructies. Bij problem-oriented-policing is er specifieke aandacht voor het identificeren van problemen in specifieke 'target areas'. Bij offender-focused policing werd de politie ondersteund door de Central Intelligence Unit (CIU). De laatstgenoemde interventiestrategie bleef het effectiefst te zijn. De onderzoekers stelden vast dat in de hotspots waar deze strategie werd ingezet de geweldsmisdrijven met 22 procent afnamen. Bij deze strategie was er een belangrijke rol weggelegd voor de CIU. Uit een recenter artikel bleek dat de 'offender focus' een reductie van geweldsmisdrijven van 42 procent werd gemeten. De 'offender focus strategy' bleek in belangrijke mate van invloed te zijn op deze resultaten. Een onderdeel van deze strategie was de toewijzing van verbindingsofficieren van criminele inlichtingendiensten aan districten (Groff e.a., 2015).

Pilot predictive policing Shreveport Police Department (SPD) in Louisiana

In 2012 heeft het Shreveport Police Department (SPD) in Louisiana een pilot uitgevoerd die een predictie- en preventiemodel omvatte met als doel om residentiële auto-gerelateerde en zakelijke eigendomsmisdrijven te reduceren. Uit een evaluatie van Hunt e.a. (2014) kwam naar voren dat deze pilot geen statisch significante reductie in eigendomsmisdrijven tot gevolg had. Daar werden verschillende verklaringen voor aangedragen. Ten eerste namen relatief weinig districten deel aan de pilot en was de tijdsduur van deelname kort. De statistische mogelijkheden om 'harde' effecten te meten waren als gevolg daarvan beperkt. Daarnaast was er binnen de districten die deelnamen aan de pilot sprake van een heterogene aanpak, bijvoorbeeld ten aanzien van interventie-strategieën in de 'hotspots' en dat bemoeilijkte het meten van de impact. De preventieve interventies werden ook in onvoldoende mate gespecificeerd en gestandaardiseerd. De politiecapaciteit om interventies uit te voeren was soms ook ontoereikend.

Pilot predictive policing Chicago Police Department

Saunders e.a. (2016) hebben onderzoek gedaan naar een pilot op het gebied van predictive policing die in 2013 werd uitgevoerd door het Chicago Police Department (CPD). Het doel van deze pilot was om wapengeweld in Chicago tegen te gaan. Om dit doel te bereiken, werd met behulp van algoritmen een Strategic Subject List (SSL) aangelegd van 426 personen waarvan werd ingeschat dat ze een hoog risico vormden ten aanzien van wapengeweld, waarna lokale politieagenten preventieve interventies ontplooiden. De mensen op de lijst konden potentiële daders of slachtoffers zijn. Bij de pilot werden vijf fasen onderscheiden, namelijk informatie verzamelen, informatie analyseren, informatie prioriteren, interventies plegen en de impact daarvan evalueren. De pilot bood inzicht in de potentiële implicaties van predictive policing programma's. Daar staat tegenover dat de pilot geen significante bijdrage heeft geleverd aan het verminderen van wapengeweld in Chicago. In dat opzicht was de pilot is Chicago geen succes. Verder bleek het lastig voor politieagenten in Chicago om de voorspellingen te vertalen naar beredeneerde preventieve activiteiten. Vaak werd de keuze gemaakt om contacten te leggen met potentiële daders en slachtoffers die op de Strategic Subjects List stonden. Dit resulteerde in een toename van persoonlijke contacten tussen politiemensen en de potentiële daders en slachtoffers die op de risicolijst stonden, maar er zijn geen concrete aanwijzingen dat intensievere persoonlijke contacten het wapengeweld in Chicago verminderen. Deze pilot toonde daarmee aan dat het uitermate lastig is om de effectiviteit van predictive policing vast te stellen. Tot slot maakte de pilot duidelijk dat het aanleggen van een risicolijst het gevaar van etnische profilering met zich meebrengt. Aandacht voor de privacy van burgers is eveneens een belangrijk aandachtpunt bij het verder uitrollen van predictive policing.

Kouziokas (2017) heeft in een afzonderlijke studie verkeersdata, criminaliteitsdata en ruimtelijke data van Chicago en het CPD gecombineerd om hotspots te voorspellen en deze voorspellingen bleken accuraat te zijn. Tot slot wees Sheehey (2019) op de 'power and politics' van algoritmen. Algoritmen zijn niet neutraal. Raciale vooroordelen kunnen volgens haar doorwerken in algoritmen die bij de SSL worden gebruikt en dat is onwenselijk.

Predictive policing in Los Angeles en Kent

Mohler e.a. (2015) hebben toepassingen van predictive policing die worden gebruikt door de politie in Los Angeles (Verenigde Staten) en Kent (UK) onderzocht. De onderzoekers constateerden dat het bijna realtime 'Epidemic-Type Aftershock Sequence (ETAS) systeem, waarbij gebruik wordt gemaakt van voorspellende algoritmen, accurater en beter in staat is om risico's op het gebied van criminaliteit te voorspellen en criminaliteit te verminderen in vergelijking met handmatige handelingen van misdaadanalisten (Mohler e.a., 2015). In het onderzoek werd een bescheiden reductie (gemiddeld 7,4 procent) van criminaliteit in hotspots als gevolg van predictive policing waargenomen. De onderzoekers verwachten dat wanneer op basis van predictive policing dynamische politiepatrouilles worden uitgevoerd de criminaliteitsreductie in hotspots aanzienlijk kan zijn. Dynamisch handelen is belangrijk omdat hotspots geen statische risicoplekken zijn. Daarnaast verwachten de onderzoekers een sterkere daling van criminaliteit wanneer de voorspellende algoritmen verbeterd worden.

Predictive policing in New York

Levine e.a. (2017) hebben de toepassing van predictive policing door het New York Police Department (NYPD) in kaart gebracht. Het NYPD is de grootste lokale politiemacht in de Verenigde Staten. Het Domain Awareness System (DAS) van het NYPD is een stadsbreed netwerk van sensoren, databases, apparaten, software en infrastructuur dat besluitvormers informeert door analyses en op maat gemaakte informatie aan te leveren via smartphones en desktops van politieagenten. De ontwikkeling van DAS startte in 2008. Nadien heeft het NYPD het systeem gebruikt om een unieke combinatie van analyse- en informatietechnologie te maken, waaronder patroonherkenning, machine learning en datavisualisatie. DAS-software is ook verkocht aan andere politieorganisaties in de Verenigde Staten. Het efficiënter inzetten van personeel als gevolg van DAS heeft een geschatte besparing van 50 miljoen dollar per jaar opgeleverd. Het belangrijkste is dat het NYPD DAS heeft gebruikt om terrorisme te bestrijden en de effectiviteit van misdaadbestrijding te verbeteren. Sinds DAS in 2013 werd ingezet, is de totale criminaliteitsindex in de stad volgens de onderzoekers met zes procent gedaald.

Predictive policing in Los Angeles

Brantingham e.a. (2018) hebben data uit experimenten met predictive policing (PredPol[4]) van de politie in Los Angeles bestudeerd. De onderzoekers hebben daarbij specifiek aandacht besteed aan eventuele biases richting etnische minderheden die op kunnen treden als gevolg van het gebruik van predictive policing algoritmen. Ze constateerden dat er zorgen bestaan ten aanzien van predictive policing algoritmen die discriminerende gevolgen kunnen hebben voor etnische minderheden, wanneer politiepatrouilles in gebieden met etnische minderheden geïntensiveerd worden. In hun studie zijn echter geen significante verschillen gevonden tussen het aantal arrestaties van individuen uit minderheidsgroepen op basis van predictive policing ten opzichte van reguliere politiepraktijken. Wel werden er meer arrestaties verricht op de locaties die op basis van algoritmen werden aangewezen, maar dat is het gevolg van de hogere criminaliteitscijfers op deze plekken. Desondanks

[4] Inmiddels is PredPol gestopt, omdat de effectiviteit tegenviel.

wijzen de onderzoekers op het belang dat de politie alert is en blijft zodat 'biased arrests' voorkomen kunnen worden.

Predictive policing in Durham

De Engelse politie staat onder druk om meer te doen met minder capaciteit en om middelen efficiënter in te zetten, en om bedreigingen proactief te identificeren. Algoritmische tools beloven de besluitvormings- en voorspellingscapaciteiten van een politie te verbeteren door beter gebruik te maken van gegevens (inclusief intelligentie), zowel van binnen als buiten de organisatie. In dit artikel van Oswald e.a. (2018) wordt aandacht besteed aan de Harm Assessment Risk Tool (HART) van de Engelse politie in Durham die is ontwikkeld in samenwerking met de Universiteit van Cambridge. HART is één van de eerste algoritmische modellen die wordt ingezet door de Engelse politie. In HART worden drie risicoprofielen van potentiële daders onderscheiden, namelijk low risk, moderate risk en high risk. In het model worden 34 voorspellende variabelen gebruikt, waarbij de meeste factoren betrekking hebben op het historische criminele trackrecord van deze personen. De auteurs van het artikel hebben gekeken welke lessen uit het HART-model getrokken kunnen worden. Ze zijn tamelijk kritisch over het gebruik van algoritmische tools binnen de politie vanuit een maatschappelijke en juridisch perspectief. De gesignaleerde risico's zijn onder meer het gevaar van biases en discriminatie en de aantasting van privacy en autonomie. In het artikel wordt een consistente, evidence-based besluitvorming bepleit in plaats van 'experimentele' besluitvorming.

Compstat in de Verenigde Staten

Benbouzid (2019) heeft de toepassing van predictive policing in de Verenigde Staten onderzocht door het Compstat systeem aan een analyse te onderwerpen. Predictive policing werd in dit artikel benaderd als een managementtool die beoogde om de productiviteit en de legitimiteit van de politie te verhogen. Tegelijkertijd werd in dit artikel gewezen op de risico's die kunnen optreden wanneer aan predictive policing toepassingen discriminerende biases ten grondslag liggen. Dergelijke biases kunnen resulteren in discriminatie van etnische minderheden en dat is ongewenst. Handelen op basis van biases verlaagt de legitimiteit van de politie. Uit deze studie blijkt echter dat de activiteiten die de politie ontplooit op basis van productive policing niet meer of minder discriminerend zijn dan bestaande praktijken binnen reguliere politiepatrouilles.

Predictive policing in Chicago, New Orleans & Maricopa County

Richardson e.a. (2019) hebben het gebruik van 'dirty data' ten behoeve van predictive policing onderzocht aan de hand van empirische cases in Chicago, New Orleans en Maricopa County. In alle drie bestudeerde cases was er sprake van dirty data. Het gebruik van 'dirty data' is problematisch omdat in dat geval onwenselijke data ten grondslag liggen aan predictive policing en dat kan resulteren in voorspellingen waar zaken als bias en discriminatie aan ten grondslag liggen (zie ook: Dixon, 2021). Om die reden bepleiten de onderzoekers dat predictive policing op een zorgvuldige manier gebruikt moet worden.

KrimPro bij politie van Berlijn

Meijer e.a. (2021) hebben onderzoek gedaan naar het gebruik van het systeem KrimPro door de Berlijnse politie. Met behulp van een predictive policing systeem kunnen geografische analyses worden gemaakt van criminaliteitspatronen op basis waarvan politiecapaciteit effectiever en gericht kan worden gealloceerd naar risicogebieden. Er waren ook kritische geluiden te horen. Zo werd KrimPro door lokale politie-eenheden ervaren als een 'black-box'. Daarnaast ervaarden ze een sterke hiërarchische druk om opvolging te geven aan de adviezen van KrimPro en dit systeem 'blind' te

gebruiken. De onderzoekers spreken in dat kader over de 'algorithmic cage' waarbij macht wordt uitgeoefend op basis van het algoritmisch systeem dat KrimPro heet. Deze situatie werpt een drempel op om de informatie uit dit systeem te controleren op basis van andere contextuele en informele informatie binnen de Berlijnse politie. In Berlijn is er dus weinig ruimte om af te wijken van de adviezen en is de dominante norm dat het systeem gebruikt moet worden. Als spiegelcasus hebben de onderzoekers ook een Amsterdamse casus bestudeerd, namelijk het Criminaliteit Anticipatie Systeem (CAS) van de politie Amsterdam. Dit is een vergelijkbaar systeem als KrimPro. Een verschil is dat het systeem in Amsterdam minder 'dwingend' wordt ingezet en de bevindingen uit het systeem als aanvullend worden benaderd op de kennis van specialisten binnen de politie. Het uitgangspunt in Amsterdam is dat de informatie uit CAS een aanvulling is op de professionele kennis van deze specialisten. Daarom typeren de onderzoekers het CAS als 'the algorithmic colleaque'. De vergelijking tussen beide systemen laat zien dat vergelijkbare systemen een verschillende impact kunnen hebben op politieorganisaties. De organisatiecontext is dus een relevante factor.

Predictive policing in Duitsland en Zwitserland

Egbert & Leese (2021) hebben predictive policing onderzocht aan de hand van twee casestudy's, namelijk de politie in Duitsland en Zwitserland. Hun onderzoek bevat zowel theoretische als empirische observaties. In beide landen zijn al in een relatief vroeg stadium experimenten gestart met predictive policing. In totaal hebben de onderzoekers 11 politieorganisaties bestudeerd, namelijk vier in Zwitserland en zeven in Duitsland. Zes politieorganisaties maakten tussen 2016 en 2019 gebruik van dezelfde software (PRECOBS), zodat predictive policing praktijken in verschillende contexten met elkaar vergeleken konden worden. PRECOBS is primair gericht op het voorspellen van woninginbraken. Uit het onderzoek bleek het voorspellen van criminaliteit, ondanks de gehanteerde software, een arbeidsintensief proces. Verder is gewezen op het belang van draagvlak binnen alle lagen van de politieorganisatie om de uitkomsten van predictive policing te incorporeren in dagelijkse werkpraktijken. Vanuit dat oogpunt heeft predictive policing ook implicaties op het gebied van organisatieverandering. De belangrijkste les is dat de IT-infrastructuur bij de politie moet zijn toegerust om de grote hoeveelheden data ten behoeve van predictvie policing te verwerken. Ook werd gewezen op het belang van training om analyses te kunnen uitvoeren en de resultaten daarvan goed te kunnen duiden. De onderzoekers stellen vast dat predictive policing een blijvertje is, maar spreken wel enkele zorgen uit. Data representeren niet de hele wereld en moeten daarom met een gezonde dosis scepsis worden benaderd. Ook moeten voorspellende algoritmische analyses volgens de onderzoekers altijd transparant en begrijpelijk zijn. Verder bepleiten Egbert & Leese dat er altijd sprake is van menselijke controle over systemen en dat beslissingen niet door machines, maar door mensen worden genomen. Ook moeten voorspellingen niet worden benaderd als hard bewijs, maar als een mogelijkheid. De mogelijkheden en beperkingen van predictive policing moeten zorgvuldig worden beoordeeld en afgewogen. De auteurs concluderen dat predictive policing geen alternatief is voor bestaande politiepraktijken, maar een aanvullend instrument.

Predictive policing in Oost-Java (Indonesië)

Setyan e.a. (2021) hebben in een paper een casus in Indonesië belicht, waarbij de regionale politie in Oost-Java een algoritme gebruikt om autodiefstal te voorspellen. Autodiefstal veroorzaakt in Oost-Java veel onrust en bezorgdheid. De politie heeft daarom getracht om autodiefstallen op locaties te voorspellen op basis van eerdere incidenten. Het gebruikte intelligente systeem bleek locaties van autodiefstal tamelijk nauwkeurig te kunnen voorspellen.

Predictive policing in Mexico

Cortes & Silva (2021) hebben in een artikel de inzet van AI in Mexico belicht. Mexico is een relevante casus, omdat de criminaliteit in dit land alarmerend hoog is. In het artikel worden AI-modellen belicht die gebruikt wordt om criminaliteit in stedelijke gebieden te voorspellen. De gehanteerde algoritmen blijken te resulteren in voorspellingen die behoorlijk accuraat zijn. Ethische overwegingen en privacy blijven een aandachtspunt, al hebben die mogelijk minder gewicht in Mexico, vanwege de zorgwekkende criminaliteit en de urgentie om deze criminaliteit te bestrijden. De context is dus van invloed op de ruimte die de politie heeft en krijgt om AI in te zetten.

Predictive policing in België

Anneleen Rummens promoveerde in 2021 in België op het onderwerp predictive policing. In haar proefschrift constateert ze dat predictive policing een breed begrip is en verschillende methoden kan omvatten (near repeat modelling, machine learning methods en risk terrain modelling). Ze heeft predictive policing gedefinieerd als het gebruik van historische criminaliteits- en andere data in complexe statistische modellen om te voorspellen waar en wanneer er een hoog risico is op criminele feiten, met de bedoeling proactief politiepatrouilles aan te sturen. Deze definitie heeft twee componenten, namelijk het gebruik van complexe statistische modellen om voorspellingen te doen en op basis daarvan proactieve interventies te plegen in de vorm van gerichte politiepatrouilles. Anneleen stelt vast dat politieorganisaties bij predictive policing in belangrijke mate afhankelijk zijn van historische data. Daarnaast constateert Anneleen, in lijn met onze observaties, dat het academisch onderzoek op het gebied van predictive policing achterblijft, vooral met betrekking tot de methodologische en operationele dimensies van predictive policing. Op basis daarvan is het (nog) niet mogelijk om de effectiviteit van predictive policing eenduidig en duidelijk vast te stellen.

Safe City System bij de Abu Dhabi Police

Khalaf Al Mazrouei (2022) heeft aandacht besteed aan de AI-strategie van Abu Dhabi Police. Deze casus is relevant omdat Abu Dhabi tot de veiligste steden ter wereld behoort en de inwoners erg tevreden zijn over de veiligheid in hun stad. Een concrete toepassing is Safe City System, een innovatief informatiesysteem voor prognoses en analyse met behulp van kunstmatige intelligentie en data technologieën om de besluitvorming te ondersteunen en te informeren ten aanzien van processen op alle terreinen van de politie.

3.4 Beoogde kansen

Op basis van de bestudeerde literatuur kunnen verschillende (beoogde) kansen van predictive policing worden benoemd.

Veiligheid in samenleving verhogen

De belangrijkste doelstelling van politieorganisaties is om de samenleving veilig(er) te maken. Predictive policing kan daar een belangrijke bijdrage aan leveren. Een belangrijke doelstelling van de bestudeerde toepassingen van predictive policing is om de veiligheid in wijken, dorpen, steden en landen te verhogen door criminaliteit te verminderen (Meijer & Wessels, 2019). Predictive policing kan daartoe bijdragen in de vorm van slimme voorspellende analyses waardoor risicopersonen en risicogebieden tijdig op het netvlies van de politie komen, en dit kan een preventieve uitwerking hebben (Smit e.a., 2016). De gelokaliseerde personen zijn individuen die daders of slachtoffers kunnen worden van criminaliteit (Meijer & Wessels, 2019). Tevens stelt predictive policing de politie in staat om op basis van de opgestelde risicoprofielen die zowel personen als plaatsen (hotspots) kunnen

omvatten, proactief te handelen en specifieke interventies te plegen (Saunders e.a., 2016; Sandhu & Fussey, 2021).

Effectiviteit verhogen

Een belangrijke aanname in de bestudeerde literatuur is dat predictive policing de effectiviteit van de politie verhoogt. Tot op heden is er echter weinig literatuur beschikbaar die inzicht biedt in de daadwerkelijke effectiviteit van predictive policing (Meijer & Wessels, 2019). In de literatuur wordt vaak meer aandacht besteed aan het verwachte potentieel in plaats van het gerealiseerde potentieel van predictive policing. De empirisch georiënteerde internationale literatuur waarin de resultaten van pilots of projecten op het gebied van predictive policing zijn belicht, laten in ieder geval geen eenduidige resultaten zien (Saunders e.a., 2016; Ferguson, 2017a; Oswald e.a., 2018; Brantingham e.a., 2018; Meijer & Wessels, 2019; Rummens, 2021). Daarom is de (vermeende) effectiviteit van predictive policing niet eenduidig vast te stellen.

Waar in de ene studie de criminaliteit lijkt te dalen als gevolg van predictive policing, worden in andere studies geen effecten waargenomen (Meijer & Wessels, 2019). De verwachting is wel dat de effectiviteit van predictive policing toeneemt naarmate de algoritmen verfijnder en de beschikbare technologie geavanceerder wordt (Fergusion, 2017a). De effectiviteit van predictive policing kan niet worden losgekoppeld van de context. Predictive policing is mogelijk effectiever in uitgestrekte gebieden van Los Angeles dan in het compacte stadsgebied Manhattan in New York (Ferguson, 2017b). De keuze voor passende (AI) technologie vereist dus steeds een beredeneerde lokale afweging.

Efficiëntie vergroten

Een specifieke verwachting is dat de politie op basis van predictive policing de beschikbare middelen adequater kan inzetten op de juiste plaats en op het juiste moment (Meijer & Wessels, 2019). Predictive policing kan in dat kader worden opgevat als een instrument om de productiviteit van de politie te verhogen (Benbouzid, 2019) en ervoor te zorgen dat het politiewerk efficiënter uitgevoerd kan worden (Popova, 2020; Sandhu & Fussey, 2021). Het verhogen van efficiency wordt extra belangrijk wanneer politieorganisaties in de nabije toekomst worden geconfronteerd met bezuinigingen en het politiewerk door minder mensen gedaan moet worden (Macnish e.a. in: Jahankhani e.a. 2021). Helaas is er te weinig empirische literatuur beschikbaar op basis waarvan onderbouwde uitspraken worden gedaan over de gerealiseerde efficiencyverhoging bij de politieorganisaties in het buitenland.

3.5 Mogelijke risico's

Op basis van de literatuur kunnen ook enkele (mogelijke) risico's worden benoemd.

Discriminatie

Een risico is dat interventies van de politie op basis van predictive policing (onbedoelde) stigmatiserende en discriminerende gevolgen kunnen hebben voor individuen en groepen (Meijer & Wessels, 2019; Shapiro, 2019; Amnesty International, 2020). Aan predictive policing liggen namelijk historische data ten grondslag en daar kunnen 'hidden biases' in zitten (Brantingham 2018; Degeling & Berendt, 2018; Isaac, 2018; Joh, 2018b; Richardson e.a., 2019; Shapiro, 2019; Sheehey, 2019; Rademacher, 2020; Rummens, 2021; Sandhu & Fussey, 2021; Davis e.a., forthcoming). De prominente rol van historische data is ook problematisch, omdat het verleden van een individu niet altijd gelijk staat aan zijn of haar toekomst (Spithoven & Beerends, 2019). Als mensen uit bepaalde bevolkingsgroepen oververtegenwoordigd zijn in historische data, dan kunnen deze biases worden

gereproduceerd. En dat kan resulteren in onbedoelde discriminatie (Babuta, 2018;) of 'racial profiling' (Saunders e.a. 2016). Uit empirisch onderzoek van Brantingham e.a. (2018) en Benbouzid (2019) blijkt dat dit risico in de praktijk mee lijkt te vallen. Desondanks mag dit risico niet worden veronachtzaamd en is het van groot belang om voorspellingen uit systemen te blijven onderwerpen aan kritische menselijke controle (Brayne, 2017).

Gebrek aan verantwoording & vertrouwen

Een probleem is dat de algoritmen die aan predictive policing ten grondslag liggen vaak moeilijk te doorgronden zijn (Meijer & Wessels, 2019). In dat kader kan er sprake zijn van een 'black box' (Meijer e.a., 2021). Dit kan te maken hebben met de complexiteit van algoritmen, maar ook het gevolg zijn van een gebrek aan transparantie (Joh, 2018b; Kaufmann e.a. 2019; Hung & Yen, 2021; Davis e.a., forthcoming). Als gevolg hiervan zijn interventies op basis van predictive policing ook lastiger te verantwoorden en uit te leggen aan burgers in de samenleving ('accountability gap') (Bennett Moses & Chan, 2018; Joh, 2018b; Meijer & Wessels, 2019; Davis e.a., forthcoming). Wanneer de gemaakte keuzes en interventies niet goed uitgelegd kunnen worden aan de samenleving, dan ligt het risico op de loer dat predictive policing het vertrouwen van burgers in de politie ondermijnt (Joh, 2018b). Hobson e.a. (2021) hebben onderzoek gedaan naar de mate waarin burgers vertrouwen hebben in algoritmische besluitvorming door de politie. In dat kader hebben ze gemeten of er verschil is in vertrouwen tussen algoritmische besluitvorming en besluiten die door politieprofessionals worden gemaakt. Ze concluderen dat de respondenten de algoritmische besluitvorming ervaren als minder eerlijk en gepast dan besluiten die politieprofessionals nemen. Desondanks zijn juist deze twee aspecten bepalend bij de steun voor het gebruik van algoritmes door de politie. De onderzoekers concluderen op basis van hun bevindingen dat besluitvorming die louter is gebaseerd op algoritmen het vertrouwen van burgers in de politie kan aantasten en dat de politie besluitvorming dus niet louter moet baseren op algoritmes. Yalcin e.a. (2022) hebben de mate van vertrouwen van mensen in menselijke rechters vergeleken met hun vertrouwen in algoritmische rechters. Uit hun onderzoek blijkt dat mensen in de rechtszaal meer vertrouwen hebben in uitspraken van menselijke rechters dan in uitspraken van 'algoritmische rechters'. Het vertrouwen is wel afhankelijk van de aard van de rechtszaak. Het vertrouwen is vooral laag bij rechtszaken die emotionele complexiteit met zich meebrengen (Yalcin e.a., 2022).

Schending van privacy

Op basis van predictive policing kunnen zowel risicoplekken ('hotspots') als risicopersonen worden benoemd. De personen die op risicolijsten komen te staan kunnen zowel potentiële daders als slachtoffers van criminaliteit zijn. De privacy van (onschuldige) burgers kan daarbij in het geding zijn (Perry e.a., 2013; Saunders e.a., 2016; Joh, 2018b; Oswald e.a. 2018; Brantingham e.a., 2018; Degeling & Berendt, 2018; Benbouzid, 2019; Meijer & Wessels, 2019; Kaufmann e.a., 2019; Hung & Yen, 2021). Bij toepassingen van predictive policing waarbij de focus ligt op risicogebieden ('hotspots'), is de kans op schending van privacy van burgers minder groot. Grondige evaluaties zijn noodzakelijk om de daadwerkelijke impact van predictive policing op de privacy van burgers vast te stellen (Rummens, 2021).

Foute voorspellingen en verbanden

Bij het doen van voorspellingen is er een gedegen kans op fouten (Ferguson, 2017a; Spithoven & Beerends, 2019; Hung & Yen, 2021; Sandhu & Fussey, 2021). Daarom is het belangrijk dat de menselijke professionals op hun waarde worden geschat en dat hun professionele inzichten, ervaringen en menselijke beoordelingen van situaties niet mogen worden onderschat (Spithoven & Beerends, 2019). Een menselijke bevestiging van de logica van geautomatiseerde besluiten is geen overbodige luxe. De

ruimte voor het gezonde menselijke oordeel kan variëren. De casus in Berlijn liet bijvoorbeeld zien dat er een sterke druk kan ontstaan om te vertrouwen op systemen en dat kan ten koste gaan van het professionele oordeel van politiemensen.

Arbeidsintensief proces

Het voorspellen van criminaliteit is een arbeidsintensief proces. Ondanks het feit dat AI zorgt voor een hoge mate van automatisering is er nog steeds veel handwerk vereist (Egbert & Leese, 2021). Dit betreft onder meer menselijke controle op de geautomatiseerde processen. Deze controle is van groot belang, omdat fouten in systemen ingrijpende gevolgen kunnen hebben voor (onschuldige) burgers. Het analyseren en duiden van data vereist ook specifieke vaardigheden en competenties die verworven moeten worden. Naarmate systemen slimmer en betrouwbaarder worden, zal de behoefte aan menselijke controle wellicht verminderen, maar het blijft belangrijk dat er 'humans in the loop' blijven.

3.6 Kritische succesfactoren

Bij het effectief inzetten van predictive policing door de politie moet rekening worden gehouden met verschillende factoren die in de literatuur vaak zijn genoemd. Daarbij dient te worden opgemerkt dat veel van de genoemde kritische succesfactoren onderling samenhangen en daarom niet alleen afzonderlijk, maar (ook) integraal in ogenschouw genomen worden. Transparantie is bijvoorbeeld van invloed op de acceptatie van nieuwe technologie en duidelijke richtlijnen en periodieke evaluaties kunnen ervoor zorgen dat risico's tijdig gesignaleerd en voorkomen kunnen worden.

Acceptatie door politiemedewerkers en burgers

Acceptatie van predictive policing is een belangrijke kritische succesfactor. Dit betreft in eerste instantie acceptatie van predictive policing door politiemensen zelf. Zij zullen zelf het nut van predictive policing moeten ervaren (Smit e.a., 2016). Daarom is het belangrijk dat politiemensen predictive policing enthousiast en met belangstelling benaderen en er dus voldoende intern draagvlak is (Perry e.a., 2013; Egbert & Leese, 2021). Zij zullen dus zelf moeten ervaren dat predictive policing de beoogde voordelen oplevert, namelijk het verhogen van de veiligheid door criminaliteit te verminderen en de daarmee samenhangende aspecten van het verhogen van de effectiviteit en efficiency van het politiewerk. Ook is het belangrijk dat ze realistisch verwachtingen hebben ten aanzien van predictive policing (Perry e.a., 2013). De acceptatie van predictive policing door de samenleving wordt ook in belangrijke mate bepaald door de perceptie dat dit instrument een bijdrage levert aan een effectieve en efficiënte bestrijding van de criminaliteit. Daarnaast wordt de maatschappelijke acceptatie in belangrijke mate bepaald door de wijze waarop de politie omgaat met de (potentiële) risico's van predictive policing. Innoveren is niet alleen een kwestie van nieuwe technologie invoeren, maar ook een kwestie van nieuwe technologie omarmen. Het gebruiken van nieuwe tools als predictive policing vereist dus ook een politiecultuur die daar ontvankelijk voor is (Smit e.a., 2016).

Kwaliteit en kwantiteit van data

Predictive policing veronderstelt dat de politie op grote schaal data verzamelt en koppelt (Egbert, 2019). De gedachte hierachter is dat hoe meer data bij de politie beschikbaar zijn ('big data') hoe betrouwbaarder de voorspellingen zijn. De effectiviteit van predictive policing staat en valt dus met de kwaliteit en kwantiteit van de beschikbare (historische) data in de informatiesystemen van de politie (Perry e.a., 2013; Smit e.a., 2016; Degeling & Berendt, 2018). Fouten in de data kunnen foutieve

voorspellingen tot gevolg hebben (Perry e.a., 2013). Een implicatie is dat de politie veel data moet verzamelen (Egbert, 2019). Hoe meer informatie de politie verzamelt, hoe groter de kans dat de privacy van burgers nodeloos wordt geschonden. Dit vereist een zorgvuldige en beredeneerde afweging. Daarnaast zal de politie moeten inzetten op het verbeteren van de kwaliteit van de data die verzameld wordt (Rummens, 2021).

IT-infrastructuur

Predictive policing vereist een IT-infrastructuur bij de politie die toereikend is om grote hoeveelheden data te analyseren en predictive policing software goed te laten draaien (Egbert & Leese, 2021).

Training/professionalisering/competenties

Het gebruik van slimme software op basis waarvan de politie criminele gedragingen van burgers of criminaliteit op hotspots kan voorspellen, vereist een grondige training van politiemensen zodat ze op de juiste manier met complexe datasystemen en analysetools kunnen omgaan (Benbouzid, 2019; Egbert & Leese, 2021; Macnish e.a. in: Jahankhani, 2021). Dit betreft onder meer het voeden van dergelijke systemen en het op een correcte wijze interpreteren van de voorspellingen uit deze slimme systemen. Digitale (AI) toepassingen vragen in dat kader om nieuwe vaardigheden van politiemensen (Hitchcock e.a., 2017; Raaijmakers, 2019). Deze vaardigheden zullen via trainingen verworven moeten worden.

Menselijke oordeelsvorming

Het is van groot belang dat de resultaten uit slimme predictive policing systemen onderwerp zijn van kritische menselijke oordeelsvorming, zeker in het licht van de reeds genoemde biases die (onbedoeld) in historische datasets kunnen sluipen (Meijer e.a., 2021). Veiligheid en politiewerk zijn namelijk niet volledig te 'dataficeren' (Smit e.a., 2016). Uit de bestudeerde cases blijkt dat de ruimte voor het professionele oordeel van informatiespecialisten per toepassing kan variëren. Deze ruimte is van invloed op de mate van acceptatie van predictive policing door politieprofessionals. Een fundamentele vraag is of de politie primair vertrouwt op slimme systemen of de professionaliteit, kennis, kunde en ervaring van politiemensen. Idealiter vullen techniek en systemen elkaar aan, maar in de politiepraktijk hoeft dat niet het geval te zijn. Uit de bestudeerde cases bleek namelijk dat er bij sommige politieorganisaties sprake lijkt te zijn van een groter vertrouwen in systemen, terwijl bij andere politieorganisaties een groter gewicht werd toegekend aan het 'gezonde verstand' van politie professionals. Zowel systemen als mensen kunnen fouten maken, dus daarom is het raadzaam om niet eenzijdig systemen of mensen te vertrouwen en de uitkomsten kritisch en zorgvuldig aan elkaar te spiegelen, om de kans op fouten te verkleinen.

Transparantie

Bij predictive policing is transparantie een belangrijke kritische succesfactor (Isaac, 2018; Petit, 2018; Kaufmann e.a., 2019; Asaro, 2019). Dit betreft zowel interne als externe transparantie. Voor wat betreft de interne transparantie is het belangrijk dat politieprofessionals de data en de doelen van de analyses die aan predictive policing ten grondslag liggen, begrijpen. Interne samenwerking tussen politieagenten en informatieanalisten is daarom belangrijk (Perry e.a., 2013). Bij predictive policing is transparantie een grote uitdaging, omdat databases en algoritmen die de basis vormen van predictive policing geavanceerd en complex zijn. Als gevolg daarvan kan het zelfs voor professionals en experts lastig zijn om de uitkomsten te begrijpen en te duiden (Kaufmann e.a. 2018). Hoe intelligenter de systemen worden, hoe groter de kans dat het op een gegeven moment ook voor softwareprogrammeur niet meer goed inzichtelijk is hoe algoritmen tot bepaalde uitkomsten komen

(Kaufmann e.a. 2018). In dat kader kunnen predictive policing systemen ook ervaren worden als een black box (Petit, 2018; Meijer e.a., 2021). Voor politieorganisaties is het van groot belang dat interventies verantwoord en uitgelegd kunnen worden richting de samenleving (Raaijmakers, 2019). Dit betreft de externe transparantie. Anders is de legitimiteit in het geding en dit kan het vertrouwen in de politie ondermijnen.

Wettelijke inkadering

Een belangrijke kritische succesfactor is de wettelijke inkadering. Belangrijke juridische factoren die in de literatuur zijn benoemd in relatie tot predictive policing, zijn het rekening houden met de privacy van burgers en juridische waarborgen om (onbedoelde) discriminatie van individuen of groepen mensen te voorkomen. Tegen die achtergrond is gewezen op het belang van een juridisch kader, waarin deze factoren zijn geadresseerd (Smit e.a. 2016). Een dergelijk kader kan ook van invloed zijn op de acceptatie van predictive policing binnen de politie en de samenleving. Om predictive policing en 'algorithmic decisions systems' (ADS) op een verantwoorde manier in te zetten, zijn duidelijke richtlijnen van groot belang (Isaac, 2018). Asaro (2019) wijst op het belang van zorgvuldigheid en heeft gepleit voor een 'Ethics of Care' benadering bij het ontwikkelen van AI-systemen. Degeling & Berendt (2018) hebben bij de inzet van predictive policing gepleit voor toetsing op drie principes, namelijk een 'suitability', 'necessity' & 'proportionality' test. Verder is gepleit voor onafhankelijke regulerende autoriteiten die het gebruik van data in opsporings- en handhavingsdatabanken monitoren en op basis daarvan adviezen kunnen verstrekken of sancties opleggen (Macnish e.a. in: Jahankhani, 2021).

Periodieke evaluaties

Een leercultuur is noodzakelijk om veranderingen succesvol door te voeren (Hitchcock, 2017b). Een onderdeel van de benodigde (leer)cultuur is dat de effectiviteit van predictive policing ook regelmatig kritisch wordt geëvalueerd (Perry e.a., 2013). Bennett Moses & Chan (2018) constateren dat gepubliceerde evaluaties van predictive policing schaars zijn en bepleiten grondige en onafhankelijke valuaties om de daadwerkelijke impact van predictive policing op de misdaad en de samenleving vast te stellen en de eventuele impact beter te begrijpen.

Ontkokering

Bij predictive policing is het belangrijk dat data(bases) niet gefragmenteerd zijn en data eenvoudig gekoppeld kunnen worden ten behoeve van predictive policing analyses (Egbert & Leese, 2021). Bij centraal georganiseerde politieorganisaties is die uitdaging minder groot dan lokaal georganiseerde politieorganisaties. In Duitsland en Zwitserland is er bijvoorbeeld sprake van veel autonomie bij regionale en lokale politiekorpsen. Dit kan zorgen voor barrières bij koppelen van databases en het benutten van data buiten het eigen werkgebied.

3.7 Conclusies en reflecties

Afgaand op de definitie die in hoofdstuk 1 is gehanteerd kunnen politieorganisaties dankzij predictive policing op een intelligente manier criminele gedragingen van individuen of criminaliteit op specifieke plekken ('hotspots') voorspellen en op basis daarvan gerichte interventies plegen.

Predictive policing kan de politie helpen om criminaliteit te verminderen of te voorkomen en kan de beschikbare politiecapaciteit effectiever en efficiënter worden ingezet. De effectiviteit van predictive policing is op basis van de bestudeerde literatuur niet eenvoudig en eenduidig vast te stellen. Er zijn studies die (beperkt) effecten van predictive policing aantonen, maar ook studies die geen verschillen laten zien ten opzichte van 'traditionele' politiepraktijken. Mede in dat kader wordt er in de literatuur

gewaarschuwd voor het overschatten van het potentieel van predictive policing (Egbert, 2019). Het echte potentieel kan inzichtelijk worden gemaakt door de ervaringen met predictive policing systematischer te monitoren en te evalueren.

De inbreuk op privacy en discriminatie van burgers zijn in de literatuur vermeld als de grootste risico's van predictive policing. Dit zijn risico's op macroniveau. Desondanks zijn er in de bestudeerde artikelen (nog) geen concrete aanwijzingen gevonden dat predictive policing in de praktijk ook leidt tot (onbedoelde) discriminatie van personen of (minderheids)groepen (Brantingham e.a. 2018; Benbouzid, 2019). Eventuele fouten en een gebrek aan transparantie zijn eveneens benoemd als mogelijke risico's. Wanneer deze twee risico's daadwerkelijk optreden dan kan dit het vertrouwen van burgers in de politie aantasten en daarmee de legitimiteit van de politie worden ondermijnd. Tegelijkertijd liggen bij traditionele politiepraktijken ook fouten op de loer en kunnen onschuldige burgers ten onrechte als verdacht worden aangemerkt door agenten tijdens een surveillanceronde.

Om predictive policing effectief en efficiënt in te zetten, is het noodzakelijk dat aan verschillende kritische succesfactoren wordt voldaan. De eerste factor is maatschappelijke acceptatie (macroniveau) en acceptatie van predictive policing door politiemensen (microniveau). Zij zullen de voordelen van predictive policing dus zelf als zodanig moeten ervaren. Dat geldt overigens ook voor de politieorganisatie als geheel (mesoniveau). De politiecultuur moet dus ontvankelijk zijn voor innovaties en nieuwe werkwijzen binnen de organisatie (Norton, 2013). Transparantie is daarbij een belangrijke randvoorwaarde en tegelijkertijd een grote uitdaging op mesoniveau, omdat predictive policing systemen naar verwachting steeds intelligenter en dus ook complexer worden. Een derde kritische succesfactor is dat de politieorganisatie (mesoniveau) beschikt over veel en betrouwbare data. Hoe meer data, hoe betrouwbaarder de voorspellingen naar verwachting zijn. Dit vergroot wel de kans dat de politie ook (meer) privacygevoelige data gaat verzamelen en dat kunnen individuele burgers als knelpunt ervaren (microniveau). In dat kader is in de literatuur een brede maatschappelijke discussie bepleit over het gebruik van big data door uitvoeringsorganisaties (WRR, 2016; Spithoven & Berends, 2019). In die politieke en maatschappelijk discussie (op macroniveau) zal aandacht moeten worden besteed aan juridische, filosofische en ethische overwegingen bij de toepassing van AI om het politiewerk te ondersteunen (Norton, 2013; Smit e.a., 2016; King e.a., 2019; Popova, 2020). Het effectief en efficiënt inzetten van predictive policing vereist ook specifieke kennis en competenties van politiemensen (microniveau) en dus ook voldoende training om deze kennis en competenties te verwerven. Dit is een uitdaging op mesoniveau voor potentiële politieprofessionals en mensen die reeds bij de politie werkzaam zijn. Bij de werving van nieuwe mensen zullen dus mogelijk andere competentieprofielen opgesteld moeten worden. Bij de scholing van nieuwe medewerkers en de bijscholing van bestaande medewerkers zullen de benodigde kennis en competenties overgedragen moeten worden. Innoveren binnen de politie heeft dus ook belangrijke implicaties voor HRM. Een ander aandachtspunt is dat er ook voldoende ruimte blijft voor het professionele oordeel en gezond verstand van politiemedewerkers en dat dus niet blind wordt vertrouwd op predictive policing systemen. Deze systemen staan niet boven mensen, maar vullen hen idealiter aan. Uit de bestudeerde cases blijkt dat politieorganisaties in het buitenland daarbij op zoek gaan naar een passende balans tussen het vertrouwen op techniek en het vertrouwen op professionals.

Tot slot wordt vanuit de wetenschap gepleit voor meer veldexperimenten en comparatief onderzoek (Rummens, 2021) zodat de daadwerkelijke effectiviteit van predictive policing bij verschillende politieorganisaties nog beter gemeten en vergeleken kan worden. Idealiter worden deze onderzoeken uitgevoerd door onafhankelijke externe partijen en worden de opgedane lessen in ieder geval breed verspreid binnen de politieorganisatie.

Hoofdstuk 4: Smart Policing/Smart Surveillance

4.1 Inleiding

De inzet van slimme apparaten om online en offline de publieke ruimte te monitoren, neemt wereldwijd toe (Kasat e.a., 2019). Daarbij kan concreet gedacht worden aan slimme bewakingscamera's, Facial Recognition Technology (FRT), social media monitoring, slimme flitspalen en overige Smart Policing Initiatives(SPI). In de literatuur wordt in dat kader gesproken over smart policing of 'smart surveillance'. Smart surveillance is vaak gebaseerd op het verzamelen en analyseren van beelden en data met behulp van sociale media, sensoren en camera's. Deze data kunnen zelf worden verzameld, maar er kunnen ook data uit andere (digitale) informatiebronnen worden gebruikt. In de literatuur wordt in dat verband de term 'big data' gehanteerd. Zoals reeds is aangegeven is er sprake van een overlap tussen de genoemde thema's. Smart surveillance heeft bijvoorbeeld raakvlakken met predictive policing. Richards (2013) stelde vast dat we in "The Age of Surveillance" leven en dat zowel autocratische als democratische regimes uiteenlopende technologieën inzetten om (digitale) surveillance activiteiten te ontplooien om de handel en wandel van burgers in de gaten te houden. In democratische landen kreeg (smart) surveillance een impuls na de terroristische aanslagen in New York (2001) en Londen (2005). Richards betoogde dat niet alleen overheidsorganisaties, maar ook private bedrijven op toenemende mate persoonlijke data van burgers/klanten verzamelen en gebruiken. Bij overheidsorganisaties wordt veiligheid als belangrijk motief opgevoerd, terwijl bij bedrijven commerciële overwegingen een rol spelen en data van consumenten worden gebruikt voor gerichte marketingsactiviteiten. Feldstein (2019) wees eveneens op de gevaren van het verzamelen van grote hoeveelheden (beeld)materiaal door autoritaire regimes om nieuwe vormen van repressie en onderdrukking te creëren, zoals het inzetten van desinformatie om opponenten onschadelijk te maken. Net als Richards stelt ook Feldstein vast dat het misbruik van data ten behoeve van AI-systemen niet alleen op de loer ligt bij autoritaire regimes, maar ook bij democratische overheden.

Petit (2018) constateerde dat we nabij een "perfect surveillance and enforcement world" zijn aanbeland. Deze observatie verdient een nuancering. Net als bij predictive policing kan bij smart surveillance de mate van intelligente variëren per toepassing. De bestudeerde cases in de internationale literatuur op het gebied van smart surveillance kunnen dus variëren van 'basic' toepassingen tot het gebruik van 'very smart' apparaten. Hoe intelligenter de toepassingen, hoe groter de impact op de samenleving en de politieorganisatie naar verwachting zal zijn.

In paragraaf 4.2 wordt het concept smart surveillance nader gedefinieerd. In paragraaf 4.3 worden concrete toepassingen van smart surveillance in het buitenland beschreven. In paragraaf 4.4 worden de beoogde kansen belicht en in paragraaf 4.5 de mogelijke risico's. In paragraaf 4.6 zijn de kritische succesfactoren in kaart gebracht. In paragraaf 4.7 worden de conclusies en reflecties gepresenteerd.

4.2 Het begrip smart surveillance

Smart surveillance is een diffuus containerbegrip. Het monitoren van verdachte activiteiten in de publieke ruimte of online (cybercrime) wordt in de internationale literatuur omschreven als 'smart surveillance'. Naast smart surveillance worden in de literatuur ook de begrippen smart law enforcement (Rademacher, 2020), smart policing (Moon e.a., 2017), smart/remote sensing (Kumar et al., 2014) en big data surveillance (Brayne, 2017) gebruikt. Het Rathenau Instituut (2019) typeert de huidige maatschappij daarom als de sensorsamenleving.

Onder het begrip smart surveillance worden verschillende toepassingen geschaard. De belangrijkste daarvan zijn slimme (bewakings)camera's, Facial Recognition Technology, social media monitoring en slimme detectieystemen. Slimme (bewakings)camera's zijn camera's die voortdurend de omgeving scannen, zoals automatische kentekenlezers en camera's die publieke ruimtes monitoren om verdachte situaties te signaleren. Bij Facial Recognition Technology (FRT) is technologie die de politie helpt bij het identificeren van (verdachte) personen. Dit gebeurt door middel van een analyse van de geometrische kenmerken van het gezicht door een algoritme door het vergelijken van de vastgelegde afbeelding en één die al is opgeslagen, bijvoorbeeld van een sociale media-account. Social media monitoring wordt ingezet om verdachte activiteiten van individuen en groepen in de gaten te houden, omdat deze activiteiten kunnen leiden tot criminele gedragingen. Slimme detectiesystemen worden ingezet om meerdere verkeersovertredingen van verschillende voertuigen tegelijk te meten, bijvoorbeeld snelheidsovertredingen, onvoldoende afstand bewaren, door rood licht rijden, verkeerd inhalen, de vluchtstrook gebruiken of mobiele telefoons vasthouden. Multifunctionele flitspalen worden ook wel superflitspalen genoemd.

Uit deze voorbeelden blijkt dat de politie bij smart surveillance gebruik kan maken van statische en mobiele apparaten. Daarnaast kan een onderscheid worden gemaakt tussen slimme apparaten die beelden en/of geluiden registreren, en software om de verzamelde data te analyseren zodat verdachte activiteiten van individuen en groepen (tijdig) kunnen worden gesignaleerd. Verder kan een onderscheid worden gemaakt tussen apparaten en technieken die al dan niet autonoom handelen. Een slimme flitspaal kan zelf overtredingen signaleren, boetes bepalen en mogelijk ook op een geautomatiseerde manier verwerken. Op deze wijze worden niet alleen overtredingen gesignaleerd, maar daar ook meteen acties aan verbonden namelijk sancties in de vorm van boetes. Als het systeem alleen verkeersovertredingen signaleert en sanctioneert is sprake van een beperkte, taakspecifieke intelligentie. Op het moment dat de flitspalen ook andere delicten signaleren, bijvoorbeeld onverzekerde voertuigen of verdachte personen in voertuigen, dan is de benodigde intelligentie hoger.

4.3 Concrete toepassingen in het buitenland

In deze paragraaf worden concrete toepassingen bij de politie in het buitenland belicht. Dit betreft respectievelijk slimme bewakingscamera's, Facial Recognition Technology, social media monitoring en Smart Policing Initiatives.

4.3.1 Slimme bewakingscamera's

Kasat e.a. (2019) hebben in een artikel aandacht besteed aan een AI-applicatie die kan worden gebruikt om abnormaal gedrag te herkennen bij het analyseren van beelden die met bewakingscamera's worden gemaakt. Het betreffende systeem (Kinect Sensor) kan bepaalde lichaamshoudingen in verband brengen met abnormale of verdachte gedragingen van personen, bijvoorbeeld diefstal of agressiviteit. De onderzoekers concluderen dat het systeem wel moet worden gevoed met veel data zodat het systeem op basis daarvan getraind wordt en op deze manier betrouwbare resultaten oplevert. In het artikel worden geen uitspraken gedaan over de effectiviteit van deze applicatie in de praktijk. Er zijn raakvlakken met FRT, zeker wanneer mensen met verdachte gedragingen gekoppeld kunnen worden aan verdachte personen. Verdachte gedragingen hoeven uiteraard niet automatisch re resulteren in criminele gedragingen. Nerveus gedrag kan bijvoorbeeld verschillende oorzaken hebben. Iemand met straatvrees kan bijvoorbeeld regelmatig achteromkijken, terwijl deze persoon geen kwade bedoelingen heeft.

4.3.2 Facial Recognition Technology (FRT)

FRT in het Verenigd Koninkrijk

Purshouse & Campbell (2019) hebben het gebruik van FRT in het Verenigd Koninkrijk (namelijk Engeland en Wales) bij outdoor festivals, sportevenementen en publieke protesten onderzocht. Zij hebben daarbij drie politieorganisaties onderzocht, namelijk Leicester Police, South-Wales Police (SWP) en de Metropolitan Police Service (MPS). De onderzoekers constateren dat privacy- en mensenrechten nog onvoldoende werd onderkend door de politie in Engeland en Wales bij de toepassing van FRT. Daarnaast problematiseren ze het gebrek aan transparantie ten aanzien van het selectieproces, waardoor het niet duidelijk is op basis van welke criteria personen op een watch list belanden. Biases kunnen daarbij een rol spelen, als gevolg waarvan mensen met specifieke etnische kenmerken onterecht als verdachte personen worden gevolgd door de politie. Verder hebben we gewezen op het belang van kwalitatief hoogwaardige beelden. Een lage beeldkwaliteit heeft geresulteerd in een groot aantal vals positieven bij de toepassing van FRT tijdens de Champions League finale van 2017. De onderzoekers constateren dat er nog te weinig reflectie is op de doelen en (on)bedoelde gevolgen van de inzet van FRT door de politie in Engeland en Wales. Ze bepleiten daarom duidelijke richtlijnen ('Codes of Practice') en nationale wettelijke kaders bij het inzetten van FRT. Daarnaast bepleiten ze een terughoudende inzet van FRT. Volgens hen moet FRT alleen bij serieuze bedreigingen van de openbare veiligheid worden ingezet.

FRT in Londen

Fussey & Murray (2019) hebben tien testen met live facial recognition (LFR) technology bij de Metropolitan Police Service (MPS) in Londen bestudeerd die werden uitgevoerd tussen 2016 en 2019. In hun onderzoeksrapport constateren ze dat een expliciete juridische basis ontbreekt op basis waarvan de inzet van deze technologie kan worden gelegitimeerd. In dat kader hebben Fussey & Murray gepleit voor een nationaal debat over juridische vraagstukken. Fussey et al. (2021) hebben nadien wederom onderzoek gedaan naar het gebruik van FRT door de Metropolitan Police Service (MPS) in Londen. De onderzoekers uiten hun zorgen over de discretionaire ruimte om te bepalen wie er op de watch list staan. Het is belangrijk dat daar voldoende ruimte is voor het professionele oordeel van politieprofessionals. Om die reden bepleiten de onderzoekers 'assisted facial recognition' in plaats van 'automated facial recognition'. Bij de eerstgenoemde toepassing worden professionals ondersteund door de technologie en heeft het professionele oordeel van politieprofessionals meer gewicht bij het bepalen van mensen die op de watch list komen te staan dan bij geautomatiseerde gezichtsherkenning. Verder constateren ze dat vooralsnog een expliciete legale basis ten aanzien van het gebruik van FRT door de MPS ontbreekt. Mede daarom bepleiten ze een nationaal debat ten aanzien van de legale basis van FRT en mensenrechten die in het geding kunnen zijn.

FRT in China, Duitsland, Verenigd Koninkrijk en Verenigde Staten

Kostka et al. (2021) hebben onderzocht hoe burgers FRT ervaren. Zij hebben daarbij vier verschillende politieke contexten vergeleken (China, Duitsland, Verenigd Koninkrijk en Verenigde Staten). De mate waarin overheidsgeleide FRT-systemen geïmplementeerd worden, verschilt aanzienlijk tussen de vier landen. In de Verenigde Staten en het Verenigd Koninkrijk worden de mogelijkheden van slimme gezichtsherkenning volop getest.[5] Dat geldt in sterkere mate ook voor China. Duitsland is echter

[5] Een concreet Amerikaans voorbeeld is het inzetten van FRT door de FBI bij het identificeren van personen die betrokken waren bij de bestorming van het Capitool in januari 2021. Zie: https://spectrum.ieee.org/facial-recognition-and-the-us-capitol-insurrection.

terughoudender met de inzet van video surveillance. Daar liggen historische redenen aan ten grondslag, namelijk de totalitaire politiestaat onder het naziregime (Rademacher, 2020). De studie van Kostka et al. (2021) laat zien dat FRT het meest geaccepteerd wordt door respondenten uit China[6] en het minst door respondenten uit Duitsland.

FRT in Verenigde Staten, Verenigd Koninkrijk en Europese Unie

Almeida e.a. (2021) hebben vergelijkend onderzoek gedaan naar de ethiek van FRT in de Verenigde Staten, het Verenigd Koninkrijk en de Europese Unie. Ze constateren dat de opmars van FRT complexe ethische afwegingen vereist tussen individuele privacy en collectieve sociale veiligheid. De opmars van FRT is in de Verenigde Staten groot, omdat de juridische kaders aldaar minder nadruk leggen op databescherming en privacy. In het Verenigd Koninkrijk en de Europese Unie speelt privacy een belangrijke rol. In de Europese Unie spelen het EVRM, de AVG en het principe van Privacy bij Design een belangrijke rol. De onderzoekers constateren verder dat er geen internationale regulatieve kaders zijn die de toepassing van FRT reguleren. Ze bepleiten dat data protection impact assessments (DPIA) en human rights impact assessments, evenals meer transparantie, regulering, audits en uitleg over het gebruik van FRT en de toepassing in individuele contexten, de implementatie van FRT ten goede zou komen.

AFR bij South Wales Police Force (SWP)

Keenan (2021) heeft in een artikel een juridische zaak belicht die was aangespannen tegen de South Wales Police Force (SWP). De SWP is in het Verenigd Koninkrijk een voorloper op het gebied van de toepassing van Automated Facial Recognition Technology (AFR). Medio 2017 werd AFR voor het eerst ingezet door de SWP tijdens de finale van de Champions League in Millennium Stadium in Cardiff. Bij AFR wordt een database op basis van bestaande beelden een watch list opgesteld. De burger die de zaak aanspande, beklaagde zich over het feit dat zijn gezicht werd gedetecteerd en verwerkt in AFR op twee verschillende momenten en dat dit een inbreuk was op zijn privacy. Het Hof van Beroep oordeelde dat het gebruik van AFR op drie gronden onwettig was. Deze uitspraak kan gevolgen hebben voor de toepassing van AFR door andere organisaties.

Het potentieel van beeldherkenning om kindermisbruik te traceren

Phippen & Bond (in: Jahankhani e.a., 2021) hebben een beschouwend artikel geschreven over de mogelijkheden, ethiek en rechten op het gebied van beeldherkenning van kindermisbruik. Beide onderzoekers concluderen dat beeldherkenning een complexe aangelegenheid is en dat kan deze tool minder effectief maken dan men verwacht. Een gebrek aan geschikte trainingsdata kan een rol spelen, evenals 'biases'. Het is ook lastig om kindermisbruik te vertalen naar algoritmen. Bij naaktfoto's van kinderen is het bijvoorbeeld de vraag of hier al dan niet sprake is van misbruik. De kans op 'false positives' is dus hoog. De onderzoekers bepleiten daarom evaluaties om beeldherkenning beter te begrijpen (Phippen & Bond in: Jahankhani e.a., 2021).

4.3.3 Social media monitoring

De politie kan sociale media monitoren om relevante informatie te verzamelen. AI kan daarbij worden ingezet om relevante trends en patronen inzichtelijk te maken (King e.a., 2019). Veel van de hieronder vermelde bijdragen hebben niet betrekking op een specifiek land, maar hebben een generieke insteek.

[6] Er kunnen vraagtekens worden geplaatst bij dergelijke surveys, omdat de respondenten sociaal wenselijke antwoorden kunnen geven.

Digitaal grasduinen op internet

In een (generieke) beschouwende bijdrage wees Richards (2013) op de gevaren wanneer overheden (en bedrijven) op onbeperkte schaal “internet surveillance” plegen, omdat de gevaren van misbruik heel groot zijn. Van misbruik is bijvoorbeeld sprake wanneer individuele burgers zonder gegronde verdenkingen op sociale media intensief gevolgd worden. Hun (intellectuele) privacy kan dan in het geding zijn.

Benutting van open source communicatie om criminele patronen inzichtelijk te maken

Williams e.a. (2017) hebben onderzoek gedaan naar de kansen en risico’s van het gebruik van open source communicatie op sociale media om criminele patronen inzichtelijk te maken en in te schatten. De onderzoekers bepleiten een theory driven big data collection, waarbij strikte checks and balances vereist zijn. Daarnaast wijzen ze op het belang om open data te verrijken met conventionele informatiebronnen van de politie en dus open en interne politiedata naast elkaar te leggen. De betrouwbaarheid van data op sociale media kan namelijk te wensen overlaten.

Big data surveillance bij LAPD

Brayne (2017) heeft kwalitatief onderzoek gedaan naar big data surveillance binnen het Los Angeles Police Department (LAPD). Ten behoeve van haar onderzoek heeft ze interviews afgenomen en observaties gedaan. Ze constateerde dat het gebruik van data bij surveillance activiteiten weliswaar geen nieuw fenomeen is, maar dat big data surveillance wel een enorme impuls heeft gekregen. In dat kader nam ze zowel een verbreding als een verdieping van (big data) surveillance waar. De verbreding betrof het passief volgen van heel veel mensen. De verdieping had betrekking op het intensiever volgen van individuen door de tijd heen. Verder constateerde Brayne dat nieuwe (digitale) surveillance technologieën ongelijkheid kan reduceren, maar ook kan vergroten. Enerzijds kan data-driven surveillance menselijke vooroordelen wegnemen, maar anderzijds kunnen biases in historische data worden gereproduceerd bij data-driven surveillance. In dat opzicht zijn historische data zelden compleet. Criminaliteit in de openbare ruimte zijn zichtbaarder voor de politie en zullen dus eerder worden geregistreerd dan minder zichtbare vormen van criminaliteit.

Sociale media benutten voor terrorismebestrijding

Pelzer (2018) heeft onderzoek gedaan naar het gebruik van sociale media ten behoeve van terrorismebestrijding. De beschikbaarheid van big data-tools voor de analyse van (beeld)materiaal op sociale media heeft geleid tot bezorgdheid over het ontstaan van door algoritmen aangestuurde profileringstechnieken die leiden tot sociale controle van grote populaties. Bij de bestudeerde tools is het belangrijk dat een onderscheid kan worden gemaakt tussen radicale en niet radicale inhoud. De meeste tools volgen een technologiegedreven aanpak die gericht is op het optimaliseren van de precisie van algoritmen. De tools missen zowel een conceptueel model van (gewelddadige) radicalisering als een duidelijke focus op het bieden van beslissingsondersteuning in termen van het helpen van menselijke analisten bij het filteren van gegevens. Het artikel stelt dat technologiegedreven benaderingen niet passen bij de huidige politiepraktijken op het gebied van terrorisme en extremisme, die gebaseerd zijn op professionele oordeelsvorming in plaats van op algoritme-gedreven patroonidentificatie in big data.

Potentieel van big data voor het politiewerk

Milosevic e.a. (2020) hebben de mogelijkheden van big data voor het politiewerk belicht, waarbij de politie data uit verschillende (openbare) bronnen, waaronder sociale media, is benut. De grootste

uitdaging is niet het verzamelen en opslaan van enorme hoeveelheden data, maar de extractie van bruikbare informatie uit big data.

Benutting van nieuwe technologie bij bestrijding van terrorisme.

Henschke e.a. (eds.) (2021) besteden in het boek *Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism* aandacht aan de inzet van nieuwe technologie bij de bestrijding van terrorisme. In het boek worden uitdagingen en belemmeringen benoemd die bij terrorismebestrijding een rol kunnen spelen. Daarnaast worden concrete technologieën besproken die kunnen worden ingezet, zoals drones, het monitoren van content op sociale media door middel van surveillance technologieën, riot control technologies, autonome wapensystemen (AWS), Facial Recognition Technology (FRT) en IoT (Internet of Things). Het IoT is een verzamelwoord voor verschillende systemen en apparaten die aan elkaar gekoppeld kunnen worden. Concrete aandachtpunten zijn ethische en morele vraagstukken, privacy, proportionaliteit, autonomie, biases in algoritmes en de afhankelijkheden ten aanzien van derde partijen die de benodigde technologieën leveren en de machtsconcentratie van technologische bedrijven.

4.3.4 Geautomatiseerde (detectie)systemen

Superflitspaal in België

In België is de eerste 'superflitspaal' in gebruik genomen in de strijd tegen verkeersovertreders.[7] Deze flitspaal wordt in eerste instantie gebruikt om te controleren of vrachtwagenchauffeurs voldoende afstand houden. De flitspaal heeft een bereik van 200 meter en kan op acht rijbanen tegelijkertijd voertuigen flitsen. Het apparaat kan verder snelheden tot 300 kilometer per uur meten en overtredingen registreren als door rood rijden, verkeerd inhalen, de vluchtstrook gebruiken of de telefoon vasthouden. Ook kan het toestel detecteren of iemand via de pechstrook een file passeert. Deze in Frankrijk vervaardigde flitspaal wordt daar al langere tijd ingezet. De flitspaal leent zich ook voor andere toepassingen, zoals nummerplaatherkenning en rekeningrijden. Dit is een voorbeeld van een technologie die in staat is om verschillende taken uit te voeren en dus een stap verder gaat dan taakspecifieke intelligentie. Het is nog te vroeg om uitspraken te doen over de ervaringen die met de superflitspaal zijn opgedaan. Wel kan worden gepleit voor een onafhankelijke evaluatie die met andere politieorganisaties worden gedeeld, zodat ook de politie in Nederland hier lessen uit kan trekken.

Algoritmische politie surveillance in België

Van Brakel (2021) besteedt in een verkennend artikel aandacht aan algoritmische politie surveillance in België en stelt de keerzijden daarvan kritisch aan de kaak, zoals de toegenomen invloed van algoritmen op de besluitvorming en de gebrekkige (democratische) controle en toezicht op deze surveillance activiteiten die tijdens de COVID-pandemie een extra impuls kregen. Daarnaast belicht ze de sociale en ethische gevolgen van 'algorithmic police surveillance'. Ze bepleit periodieke evaluaties om vast te stellen of het gebruik van nieuwe toepassingen publieke belangen blijven dienen. Tot slot bepleit ze regulering.

Automated License Plate Recognition (ALPR) in India

Kaur e.a. (2022) hebben in een verkennende reviewstudie Automated License Plate Recognition (ALPR) in India belicht. ALPR werd in 1976 ontwikkeld in het Verenigd Koninkrijk. Dit systeem kan nuttig zijn

[7] https://www.ad.nl/auto/superflitspaal-nu-ook-in-belgie-ingezet-in-de-strijd-tegen verkeersovertreders~a07f5fa5/

op verschillende terreinen, zoals traffic control, parkeren en tolwegen. Op het veiligheidsdomein biedt ALP mogelijkheden om bijvoorbeeld gestolen of verdachte voertuigen te traceren.

4.3.5 Smart Policing Initiatives

In deze paragraaf worden concrete activiteiten in de Verenigde Staten belicht die zijn uitgevoerd in het kader van Smart Policing Initiatives (SPI), evenals percepties over smart policing in andere landen.

Smart policing in Glendale

White & Katz (2013) hebben onderzoek gedaan naar een Smart Policing Initiative (SPI) van de Arizona Police Department in Glendale. Het politieteam in Glendale heeft een slimme probleemgeoriënteerde policing methode ingezet om criminaliteit en wanorde in winkels in deze stad te adresseren. Uit het onderzoek bleek dat de criminaliteit in de 'target stores' significant daalde in het jaar waarin interventies werden gepleegd. De samenwerking met private partijen bleek een belangrijke kritische succesfactor te zijn.

Smart policing in Boston

Braga & Schnell (2013) hebben onderzoek gedaan naar een Smart Policing Initiative (SPI) van de Boston Police Department (BPD) in Boston. Dit betrof 'problem-oriented policing interventions' op hotspots waar een substantieel deel van de geweldsmisdrijven plaatsvond. Het project bouwde voort op de Safe Street Teams (SST) die in 2007 werden opgericht om geweldmisdrijven op hotspots tegen te gaan. De Boston Regional Intelligence Center (BRIC) heeft op basis van 'computerized mapping technology' en criminaliteitsdata in totaal dertien hotspots geïdentificeerd waar de Safe Street Teams 'problem-oriented' interventies pleegden. Dit project heeft raakvlakken met predictive policing. Uit een evaluatie bleek dat de interventies resulteerden in een significante afname van geweldsdelicten in de betreffende hotspots in vergelijking met andere locaties. Er werden ook geen aanwijzingen gevonden dat de geweldsdelicten zich verplaatsten van de hotspots waar interventies werden gepleegd naar andere plekken.

Smart policing in Las Vegas

Baldwin e.a. (2014) hebben onderzoek gedaan naar een Smart Policing Initiative (SPI) van de Las Vegas Metropolitan Police Department (LVMPD). Bij het betreffende project werden onder meer proactieve patrouilles uitgevoerd in twaalf geïdentificeerde hotspots. In het onderzoek werd gekeken naar de impact van het project op het aantallen hulpverzoeken van burgers en de percepties over criminaliteit en politieactiviteiten. Het onderzoek liet geen eenduidige resultaten zien. Wel namen burgers meer interacties tussen politieagenten en burgers waar en dat was een belangrijk neveneffect van het project. Het project heeft raakvlaken met predictive policing.

Smart policing in Lowell

Bond e.a. (2014) hebben onderzoek gedaan naar een Smart Policing Initiative (SPI) in de stad Lowell. Bij dit project werd beoogd om drugsgerelateerde vermogensdelicten aan te pakken door middel van 'problem-oriented policing' en het zogeheten SARA-model (Scanning, Analysis, Response & Assessment). Op basis daarvan werden twaalf hotspots geïdentificeerd en vervolgens vond op deze locaties real time monitoring plaats. Het project, waarin elementen van predictive policing en smart policing zijn gecombineerd, resulteerde in een substantiële reductie van drugsgerelateerde vermogensdelicten.

Smart policing in Columbia

Wolfe e.a. (2015) hebben onderzoek gedaan naar twee Smart Policing Initiatives (SPI) in Columbia. Het Columbia Police Department (CPD) lanceerde in samenwerking met onderzoekers van de University South Carolina (USC) het Integrated Data Exchange and Analysis (IDEA) project met als doel om op basis van intelligence-led policing (ILP) woninginbraken te bestrijden. Uit een survey onder burgers bleek dat zij woninginbraken als het voornaamste probleem ervaarden. De interventie resulteerde in een daling van het aantal woninginbraken. Een ander smart policing project in Columbia betrof de toepassing van social network analysis (SNA) om de relaties tussen (vermoedelijke) bendeleden in Columbia beter te begrijpen.

Smart policing in Michigan

McGarrell e.a. (2015) hebben onderzoek gedaan naar een Smart Policing Initiative (SPI) in Michigan. Dit betrof een project van de Michigan State Police (MSP) waarbij op basis van 'data-driven' processen, 'evidence-based' praktijken en het gebruik van strategische planningen en statistieken werd getracht om de effectiviteit en efficiency van de dienstverlening aan burgers te verbeteren. Uit het onderzoek bleek dat leiderschap, kennis en vaardigheden (en dus training) en geavanceerde informatiesystemen belangrijke kritische succesfactoren zijn bij het realiseren van de benodigde organisatieverandering om de genoemde doelen te bereiken.

Smart policing in Winnipeg

Catte (2017) heeft onderzoek gedaan naar een Smart Policing Initiative (SPI) in Winnipeg. Het doel van het programma in District Oost van Winnipeg was om criminaliteits- en verkeersdata te gebruiken en proactieve policing tactieken in te zetten om de criminaliteit te doen dalen. Uit het onderzoek bleek dat leiderschap en technologie belangrijke factoren zijn bij het effectief uitvoeren van een SPI. Uit een regressieanalyse bleek dat de criminaliteit in District Oost van Winnipeg significant waren gedaald in vergelijking met andere districten.

Smart policing in Toledo

Johnson e.a. (2018) hebben onderzoek gedaan naar een Smart Policing Initiative (SPI) in Toledo. Het Toledo Police Department heeft smart policing ingezet met als doel om gewapende incidenten, overvallen en inbraken in Toledo te doen afnemen. Om dat doel te bereiken, werden de meest actieve overtreders geïdentificeerd en met behulp van een algoritme een lijst met honderd personen opgesteld waarvan de kans het grootste werd geacht dat ze een nieuwe overval, woninginbraak of zware mishandeling zouden plegen. Vervolgens ontvingen deze honderd personen een brief van de politie waarin werd gemeld dat de politie op de hoogte was van hun recente criminele gedragingen, dat ze nauwlettend in de gaten werden gehouden en dat ze bij toekomstige criminele gedragingen maximale handhaving en vervolging tegemoet konden zien. Vervolgens werd de 'awareness space' van deze personen in de gaten gehouden. Dit betreft de locaties die deel uitmaken van de dagelijkse routines van de betreffende personen. Uit criminologisch onderzoek blijkt namelijk dat daders vaak binnen deze 'awareness space' criminele activiteiten ontplooien. De onderzoekers hebben significante reducties van specifieke misdrijven waargenomen. Daarnaast bleek dat een kleine groep daders verantwoordelijk was voor een groot aantal misdrijven.

Smart policing in Verenigde Staten *en Taiwan*

Kuo & Lord (2019) hebben een cross-nationale studie uitgevoerd waarbij smart policing tussen de Verenigde Staten en Taiwan is vergeleken. De focus lag daarbij op de Data-Driven Approach to Crime and Traffic Safety (DDACTS). Bij deze benadering worden data van verkeersongevallen geïntegreerd

met criminaliteitsdata en op basis daarvan efficiëntere patrouille routes uitgezet. In de Verenigde Staten heeft deze benadering bijgedragen aan de reductie van criminaliteit en verkeersongevallen. In Taiwan bleken verkeersongevallen meer geclusterd te zijn dan criminaliteit, terwijl dat in de Verenigde Staten niet het geval was. Daar zijn verkeersongevallen vaker gerelateerd aan criminaliteit.

Percepties van publiek en politiemensen over smart policing in Zuid-Korea

Moon e.a. (2017) hebben de houding van het publiek en politiemensen in Zuid-Korea ten aanzien van smart policing technologieën die worden ingezet om cybercrime te onderzoeken en te voorkomen met elkaar vergeleken. Uit het artikel blijkt dat Zuid-Koreaanse burgers een groot belang hechten aan privacy. Dat is meteen hun voornaamste bezwaar en zorg bij smart policing toepassingen. Ook verwachten ze dat de belastingen hoger worden wanneer de politie in smart policing technologie investeert. Politiemensen hechten op hun beurt voornamelijk belang aan smart policing toepassingen vanuit de gedachte dat hun werk als gevolg hiervan minder tijd kost en dus efficiënter kan worden uitgevoerd. Er bestaan dus verschillende percepties ten aanzien van enerzijds de aanpak van cybercrime en anderzijds het inleveren van privacy ('privacy invasion'). Met beide overwegingen uit de samenleving en de politieorganisatie moet dus volgens de onderzoekers rekening worden gehouden.

Percepties van publiek in Spanje

Pavone and Esposti (2012) hebben Spaanse onderzoeksdata geanalyseerd die inzicht bieden in de wijze waarop burgers nieuwe 'surveillance-oriented security technologies' beoordelen. Hun analyse liet zien dat geen van de respondenten privacy wilde inruilen voor veiligheid aangezien bezorgde burgers aangaven dat hun privacy geschonden werd zonder dat hun veiligheid toenam, terwijl burgers die vertrouwen hebben in 'surveillance oriented security technologies' aangaven dat hun veiligheid toenam zonder dat hun privacy beïnvloed werd. De percepties van burgers kunnen dus variëren.

Percepties van burgers in Londen

Onderzoek van Bradford et al. (2020) onder volwassen burgers in Londen laat zien dat publieke acceptatie in belangrijke mate afhankelijk is van vertrouwen en legitimiteit. Daarbij lieten zij zien dat het oordeel over de politie een veel grotere voorspeller van de acceptatie is dan zorgen die men heeft over criminaliteit, wat suggereert dat de relatie met degenen die de (AI) technologie gebruiken belangrijker is dan de uitkomsten waarop de technologie gericht is.

4.4 Beoogde kansen

Op basis van de literatuur kunnen verschillende (potentiële) kansen van smart surveillance worden benoemd.

Veiligheid in samenleving verhogen

Smart surveillance op basis van AI kan de veiligheid in het publieke domein verhogen (Richards, 2013; Blount, 2017; Demir e.a., 2020). Uit empirisch onderzoek blijkt dat dankzij smart surveillance (verdachte) personen, patronen, situaties en ongewenste gedragingen (bijvoorbeeld verkeersovertredingen) tijdig kunnen worden gesignaleerd en gedetecteerd (Joh, 2016; Fan, 2018; Kasat e.a., 2019; Hood, 2020). Dergelijke 'early warning systems' kunnen zowel in de offline als de onlinewereld worden ingezet. Verdachte personen kunnen bijvoorbeeld potentiële terroristen zijn. Smart surveillance biedt daarom kansen bij terrorismebestrijding (Pelzer, 2018). Aan de hand van smart surveillance kunnen niet alleen potentiële daders worden gesignaleerd en gelokaliseerd, maar ook slachtoffers, bijvoorbeeld vermiste personen (Blount, 2017). Smart surveillance toepassingen

kunnen niet alleen de samenleving veiliger maken, maar ook het veiligheidsgevoel van politiemensen verhogen. De keuze voor en impact van smart surveillance toepassingen kan niet worden losgekoppeld van de context. In grote steden ligt bijvoorbeeld omvangrijke video surveillance meer voor de hand dan op het platteland (Ferguson, 2017b).

Kostenverlaging

Dankzij smart surveillance kan grootschalige opsporing plaatsvinden door de continue verzameling van data die door een algoritme verzameld en geanalyseerd worden. Dit leidt tot een kostenreductie voor de politie (Joh, 2015). Daar staat tegenover dat het opslaan en interpreteren van beeldmateriaal een erg kostbare aangelegenheid kan zijn (Lin, 2016).

Eerlijkere opsporing

Smart surveillance kan meer eerlijkheid in de opsporingsdiscretie introduceren. Traditioneel baseren politieagenten zich op hun vermogen om verdachte personen en gedragingen waar te nemen. Daarmee zijn beslissingen in sterke mate normatieve beoordelingen (Joh, 2015). Smart surveillance kan in potentie de normatieve beoordelingen en eventuele vooroordelen verminderen of wegnemen (Brayne, 2017). Daar staat tegenover dat aan smart surveillance algoritmen ten grondslag kunnen liggen die niet vrij zijn van discriminatie. In dat geval is geen sprake van eerlijke en onbevangen opsporing. Het kwartje kan dus twee kanten op vallen. De verwachting is wel dat de eerlijkheid van politiepraktijken stijgt en biases afnemen naarmate de beschikbare data toenemen (‘big data’) (Goel e.a., 2017). Hier is nog geen empirisch onderzoek naar gedaan.

Toepassing voor trainingsdoeleinden

Beeldmateriaal dat door de politie wordt verzameld via slimme camera’s en sensoren kan ook waardevol zijn voor trainingsdoeleinden en om te leren van elkaar (Goetschel & Peha, 2017; Fallik e.a., 2020; Demir e.a., 2020; Mrozla, 2021).

4.5 Mogelijke risico’s

Op basis van de bestudeerde literatuur kunnen ook enkele (mogelijke) risico’s van smart surveillance worden genoemd.

Schending privacy

Een risico van smart surveillance is de opkomst van een ‘surveillance culture’ (Hood, 2020), ‘total surveillance’ (Miller, 2014) of ‘mass surveillance’ (Murphy, 2018) waarin de handel en wandel van alle burgers nauwlettend wordt gemonitord en geregistreerd. Daarbij kan er sprake zijn van een (heimelijke) inbreuk op mensenrechten, zoals het aantasten van het recht op privacy en andere persoonlijke vrijheden van burgers (Richards, 2013; Lin, 2016; Brinkhoff, 2017; Bui, 2017; Hirose, 2017; Nakar & Greenbaum, 2017; Fan, 2018; Murphy, 2018; Feldstein, 2019; Joh, 2019; Purshouse & Campbell, 2019; Zeng e.a., 2019; Braga, 2020; Newell, 2020; Hood, 2020; Ferguson, 2021). Smart surveillance, bijvoorbeeld het instrument FRT, kan worden ingezet of ervaren als instrument voor staatstoezicht en -controle. Dit risico is conform het scenario van Big Brother waarbij de overheid de handel en wandel van burgers intensief volgt door middel van (slimme) camera’s, (slimme) sensoren: “more cameras and sensors will mean more watching and less freedom from being watched” (Joh, 2019a). De percepties van burgers kunnen per land variëren. Vergelijkend onderzoek van Kostka et al. (2021) laat bijvoorbeeld zien dat FRT in hoge mate wordt geaccepteerd door burgers in China en dat

de acceptatiegraad bij Duitse burgers laag is. De percepties van burgers in het Verenigd Koninkrijk en de Verenigde Staten bevinden zich daar tussenin.

Doelverschuiving

Een problematisch gegeven is dat de gegevens ook gebruikt kunnen worden voor andere doeleinden dan waarvoor ze verzameld zijn (Blount, 2017). Een concreet actueel nieuwsbericht ter illustratie: als het aan de politie in Nederland ligt, mogen beelden die voor kentekenregistratie op de snelweg worden gebruikt, ook ingezet worden om personen op te sporen.[8] in dit nieuwsbericht wordt een risico blootgelegd, namelijk dat een systeem dat voor een specifiek doel wordt ingezet (registratie van auto's) in de praktijk ook voor andere doeleinden kan worden ingezet (opsporen van personen).

Onschuldige verdachten

Een risico is dat onschuldige mensen worden gedetecteerd als verdachte personen ofwel: 'false matches' (Hood, 2020). Een lage kwaliteit van het beeldmateriaal kan het aantal 'false positive matches' verhogen (Hood, 2020; Dixon, 2021). Fouten kunnen ook optreden als gevolg van fouten in datasets of datasystemen die niet compleet of onbetrouwbaar zijn. Ook bij FRT kan onbetrouwbaarheid een knelpunt zijn, bijvoorbeeld als de kwaliteit van het beeldmateriaal te wensen overlaat (Zeng e.a., 2019). Dat is tegelijkertijd een paradox van big data: een grote hoeveelheid data wil nog niet zeggen dat deze betrouwbaar of bruikbaar zijn.

Discriminatie

Een risico van smart surveillance is 'data-driven' discriminatie van minderheden (Nakar & Greenbaum, 2017; Feldstein, 2019; Purshouse & Campbell, 2019; Hood, 2020). Ook stigmatisering kan een risico zijn, omdat bij veel surveillance toepassingen mensen in hokjes worden geplaatst (Richards, 2013; Zeng e.a., 2019). Daarnaast kan big data surveillance resulteren in sociale ongelijkheid (Brayne, 2017). De verwachting is wel dat dit gevaar afneemt wanneer de politiedata accurater worden. Big data zijn in dat kader vaak accurater dan small data (Ferguson, 2015).

Gebrek aan transparantie

Transparantie is van groot belang bij de toepassing van smart surveillance (Joh, 2019a). De mate van transparantie varieert per smart surveillance toepassing. Smart surveillance kan tot uitkomsten leiden die niet (goed) uit te leggen zijn door politieagenten of informatiespecialisten Kotsoglou & Oswald (2020). In dat kader wordt in de literatuur gesproken over de black box (Petit, 2018). FRT moet zorgvuldig en transparant worden ingezet (Zeng e.a., 2019). Het is namelijk niet altijd duidelijk op basis van welke selectiecriteria personen op een watch list worden geplaatst (Purshouse & Campbell, 2019; Fussey et al., 2021). Burgers weten ook niet altijd dat ze worden gevolgd met camera's. Op veel plekken, bijvoorbeeld op stations of in voertuigen van het OV, is het vaak duidelijk dat camera's hangen die waken over de veiligheid van reizigers. Er zijn ook veel plekken waar camera's minder zichtbaar of zelfs heimelijk worden ingezet, bijvoorbeeld de inzet van drones met camera's tijdens demonstraties, waar demonstranten zich doorgaans niet bewust van zijn. In een beschouwend artikel besteedt Feeney (2016) aandacht aan privacy in 'the Age of Policy Drones'. Drones kunnen namelijk de privacy van burgers serieus bedreigen. Een verschil met (zichtbare) bewakingscamera's is dat drones veelal onzichtbaar zijn en dus de privacy van burgers heimelijk kunnen aantasten. Feeney besteedt in zijn beschouwing aandacht aan het Vierde Amendement in de Amerikaanse grondwet die de privacy van Amerikaanse burgers beschermt tegen inbreuken op hun privacy. Tegelijkertijd zijn er smart

[8] https://www.msn.com/nl-nl/nieuws/binnenland/politie-wil-naast-kentekens-ook-personen-opsporen-met-cameras-langs-snelweg/ar-AANV5zT?ocid=entnewsntp

surveillance toepassingen die de transparantie kunnen vergroten. Het is niet altijd duidelijk wat er binnen de politie met de geregistreerde beelden gebeurt, wie er toegang tot heeft, met wie de beelden worden gedeeld en waar de beelden worden opgeslagen. Bij smart surveillance heeft transparantie dus twee gezichten. Camera's op zich zijn geen AI, maar het beeldmateriaal kan wel met behulp van AI worden geanalyseerd om verdachte personen 'automatisch' op te sporen.

Tijdrovende analyses

Het handmatig analyseren van beeldmateriaal is een tijdrovende aangelegenheid (Lin, 2016). Slimme software kan nuttig zijn om deze analyse te automatiseren, maar de teneur van de bestudeerde artikelen is dat het belangrijk is dat het professionele oordeel van politiemensen een noodzakelijk onderdeel moet blijven bij smart surveillance en dat smart surveillance dus niet louter gebaseerd moet zijn op AI.

Kostbare investeringen

Smart surveillance is een kostbare aangelegenheid en vereist grote investeringen in slimme apparaten (Lin, 2016; Bui, 2017). Goede bewakingscamera's en flitspalen zijn kostbaar, zeker wanneer deze op grote schaal worden ingezet. Dat geldt ook voor de opslag van de grote hoeveelheid beeldmateriaal dat door deze apparaten wordt verzameld. Daar staat tegenover dat smart surveillance toepassingen werk uit handen kunnen nemen en politiemensen kunnen ontlasten. Kosten en baten zullen dus per toepassing tegen elkaar moeten worden afgewogen.

Aantasting van discretionaire ruimte

Smart surveillance kan de professionele handelingsruimte van politiemensen aantasten. In de literatuur wordt in dat verband ook wel gesproken over discretionaire ruimte.

Aantasting kwaliteit van interacties

De kwaliteit van de interacties tussen burgers en politieagenten kan worden aangetast, wanneer er camera's tussen hen in zitten (Lin, 2016). Daarbij ligt het gevaar van 'dehumanization' (Miller, 2014). Nieuwe technologie kan impact hebben op de aard en toon van de interacties tussen politieagenten en burgers. Dit geldt voor gerobotiseerde systemen, maar ook voor slimme flitspalen die verkeersovertredingen registreren. Bij het staande houden van mensen kunnen politieagenten de overtredingen ter plekke toelichten, maar bij boetes op de deurmat is dat niet het geval.

Dominantie van private bedrijven

Joh (2017) stelt dat binnen de Verenigde Staten traditioneel verondersteld werd dat de politie de leiding had over hun eigen onderzoeksinstrumenten. Doordat de politie nu steeds vaker consument wordt van nieuwe opsporingstechnologie die gecreëerd en verkocht wordt door private bedrijven, is het de vraag of dit een wenselijke ontwikkeling is. Dit risico, dat overigens geldt voor alle nieuwe technologieën die de politie inzet, is overigens ook reëel in Nederland. De WRR constateerde dat Nederland in hoge mate afhankelijk is van AI-gerelateerde diensten en producten van (Amerikaanse) tech giganten (Bakker e.a., 2021). Private bedrijven krijgen daarmee een flinke invloed op de publieke politie die vaak niet erkend worden, maar die consequenties hebben voor de burgerlijke vrijheid en politietoezicht. Daarbij komt dat de private bedrijven vaak de data opslaan, omdat de politie die capaciteit niet heeft, maar daar vervolgens wel flinke bedragen voor kunnen vragen. Onlangs werd ook in een nieuwsbericht naar buiten gebracht dat er zorgen bestaan ten aanzien van het gebruik van Chinese bewakingscamera's in Nederland, waarbij het risico bestaat dat de Chinese overheid of andere

instanties mogelijkerwijs ook heimelijk kunnen meekijken met de beelden die met deze apparaten worden geregistreerd.[9]

4.6 Kritische succesfactoren

Bij het effectief inzetten van smart surveillance door de politie moet rekening worden gehouden met verschillende factoren die in de bestudeerde literatuur zijn genoemd.

Acceptatie door politiemedewerkers en burgers

Bij het implementeren van innovaties is het belangrijk dat beoogde doelgroepen en gebruikers daar ontvankelijk voor zijn (Norton, 2013). Een belangrijke factor bij de toepassing van big data surveillance is het vertrouwen dat medewerkers hebben in de data die beschikbaar is (Ferguson, 2017b). Een belangrijke factor die de impact van FRT zal bepalen is de acceptatie door burgers (Zeng e.a. 2019). Uit de reeds genoemde studie van Kostka e.a. (2021) bleek dat de mate van acceptatie afhankelijk is van de context en dus per land verschillend kan zijn.

Wettelijke inkadering

Een goed omschreven (nationaal) wettelijk kader met richtlijnen en heldere instructies op het gebied van smart surveillance is belangrijk (Richards, 2013; Blount, 2017; Nakar & Greenbaum, 2017; Feldstein, 2019; Purshouse & Campbell, 2019; Ferguson, 2021). Hierbij valt onder andere te denken aan waar de beelden worden opgeslagen, hoe lang ze worden opgeslagen, door wie en waarvoor de beelden geraadpleegd mogen worden en hoe lang de data bewaard mogen worden (Bui, 2017). Verder wordt gepleit voor regelgeving die duidelijk markeert welke data analytics al dan niet toegestaan zijn op basis van de vergaarde beelden en data (Fan, 2018; Zeng e.a., 2019). Ethics by design is een bruikbaar instrument om potentiële ethische en technische risico's tijdig te traceren (Zeng e.a., 2019). Bud (2016) constateert dat de ontwikkeling van wetgeving sterk achter ligt op de snelheid waarmee de smart surveillance technologie zich ontwikkelt.

Datakwaliteit

De impact/effectiviteit van smart surveillance is in belangrijke mate afhankelijk van de kwaliteit van het beschikbare en/of verzamelde (beeld)materiaal (Purshouse & Campbell, 2019). De kwaliteit (en kwantiteit van (beeld)data bepaalt in belangrijke mate de kwaliteit van smart surveillance. Daarmee is betrouwbaarheid een relevante kritische succesfactor bij smart surveillance (Joh, 2019). Uit de bestudeerde literatuur is gebleken dat de betrouwbaarheid van FRT nog niet optimaal is. Zo is er sprake van hoge 'error rates' bij vrouwen met een donkere huidskleur (Zeng e.a., 2019). Dergelijke fouten kunnen ingrijpende gevolgen hebben en resulteren in personen die ten onrechte op een watch list belanden.

Dataveiligheid

Het is belangrijk dat het door de politie verzamelde beeldmateriaal op veilige plekken wordt bewaard. Naarmate de hoeveelheid beeldmateriaal dat de politie verzamelt toeneemt, wordt ook dataveiligheid een steeds belangrijker issue. Deze privacygevoelige beelden moeten namelijk op een veilige manier worden gedeeld en opgeslagen binnen de politieorganisatie. Deze data mogen niet in handen komt van derden als gevolg van hacking of dataleks (Nakar & Greenbaum, 2017). Dat geldt voor beelden die slimme bewakingscamera's registeren, maar ook voor beeldmateriaal die de politie gebruikt ten

[9] https://nos.nl/artikel/2416279-omstreden-chinese-camera-s-hangen-overal-in-nederland-ook-bij-ministeries

behoeve van FRT (Zeng e.a., 2019). Deze (beeld)data moeten effectief worden beschermd tegen hackers (Nakar & Greenbaum, 2017). Data firewalls moeten data beschermen (Zeng e.a., 2019). Inmiddels zijn er meerdere incidenten geweest waarbij biometrische gegevens van burgers op straat kwamen te liggen.[10]

Debat en evaluaties

Ferguson (2017b) bepleit lokale en nationale 'surveillance summits' waarbij de ingezette big data surveillance toepassingen door de politie jaarlijks wordt geaudit, geëvalueerd en verantwoord. De technische en ethische uitdagingen moeten eveneens regelmatig worden geëvalueerd (Zeng e.a. 2019).

4.7 Conclusies en reflecties

Smart surveillance is een containerbegrip waar uiteenlopende toepassingen onder worden geschaard. In dit hoofdstuk is aandacht besteed aan slimme bewakingscamera's, FRT, social mediamonitoring, slimme flitspalen en smart policing tools.

De mate van intelligentie van de toepassingen die vallen onder smart surveillance kan variëren. Zo is er een belangrijk verschil tussen standaard camera's en flitspalen die beelden registreren en foto's maken, en de slimme software (bijvoorbeeld FRT) die wordt ingezet om een grote hoeveelheid beelden te analyseren om verdachte personen 'automatisch' op te sporen, overtredingen automatisch te sanctioneren en verdachte activiteiten online en in de publieke ruimte in kaart te brengen.

Belangrijke kansen die in de literatuur zijn benoemd, betreffen het verbeteren van de veiligheid, respectvollere interacties, kostenverlaging, eerlijkere opsporing, transparantie en verantwoording, minder klachten en toepassing voor trainingsdoeleinden. Het verbeteren van de veiligheid geldt voor de hele samenleving (macro), maar kan ook gelden voor individuen. Dankzij slimme camera's en monitoringsystemen kunnen onwenselijke of criminele gedragingen in beeld worden gebracht en daarmee burgers worden beschermd tegen mogelijk geweld of andere onwenselijke gedragingen (microniveau). Respectvolle interacties tussen politiemensen en burgers zijn niet alleen in het belang van individuen, maar ook voor de politieorganisatie (mesoniveau) en samenleving (macroniveau). Respectvolle interacties zijn namelijk belangrijk voor de legitimiteit van de politieorganisatie en het vertrouwen van de samenleving in de politie. Datzelfde geldt voor eerlijke opsporing, waarbij geen sprake is van discriminatie of vooroordelen. Kostenverlagingen zijn vooral op macro- en mesoniveau van belang, opdat van de politie mag worden verwacht dat publieke gelden op een efficiënte manier worden ingezet. Transparantie en verantwoording zijn op alle niveaus van belang. Omwille van legitimiteit en vertrouwen is het van belang dat politiewerk transparant is en dat over politieactiviteiten verantwoording wordt afgelegd richting de maatschappij en individuele burgers die het object zijn van politieactiviteiten. Transparantie en verantwoording kan er ook voor zorgen dat het aantal klachten afneemt. Klachten kunnen namelijk de reputatie van de politie ondermijnen. Het gebruik van smart surveillance toepassingen voor trainingsdoeleinden is vooral van belang op meso- en microniveau omdat deze trainingen een bijdrage leveren aan de professionalisering van de politieorganisatie en individuen die binnen deze organisaties werkzaam zijn.

Belangrijke risico's die in de literatuur zijn benoemd, betreffen schending van privacy, doelverschuiving, onschuldige verdachten, discriminatie, gebrek aan transparantie, tijdrovende

[10] https://www.bnr.nl/nieuws/technologie/10386801/ruim-een-miljoen-biometrische-gegevens-liggen-op-straat?msclkid=a6f7f964ab5d11ecb088a5cb90d77084

analyses, kostbare investeringen, aantasting van discretionaire ruimte, aantasting van kwaliteit interacties, dataveiligheid en dominantie van private bedrijven. Privacy is een individuele aangelegenheid en dus een relevante factor op microniveau. Datzelfde geldt voor doelverschuiving, onschuldige verdachten en discriminatie. Gebrek aan transparantie, kostbare investeringen, dataveiligheid en de dominantie van private bedrijven hebben vooral betrekking op het macro- en mesoniveau, omdat deze factoren van invloed zijn op het vertrouwen in en de legitimiteit van de politie. De discretionaire ruimte van politieagenten en de kwaliteit van de interacties hebben betrekking op het microniveau, namelijk individuele agenten en burgers.

Kritische succesfactoren die uit de literatuur kunnen worden afgeleid zijn acceptatie door burgers en politiemensen, wettelijke kaders, kwaliteit van het beeldmateriaal, betrouwbaarheid, dataveiligheid en transparantie. Deze kritische succesfactoren hebben betrekking op alle drie de onderscheiden niveaus. Op macroniveau is het belangrijk dat er bij smart surveillance duidelijke wettelijke kaders zijn en dat deze ook worden nageleefd. Transparantie is van belang met het oog op vertrouwen en legitimiteit. Op mesoniveau is het belangrijk dat de politie beschikt over betrouwbare en kwalitatief hoogwaardige data en beeldmateriaal, omdat dit in belangrijke mate de effectiviteit van smart surveillance bepaalt. Op microniveau is het belangrijk dat individuele burgers niet ten onrechte in risicoprofielen belanden en dat individuele privacygevoelige gegevens die via smart surveillance worden verzameld niet in handen komen van derden.

De impact van smart surveillance is op basis van de beschikbare literatuur (nog) niet goed vast te stellen. Veel bestudeerde artikelen zijn reflecterend van aard en beschrijven mogelijke kansen, bedreigingen en randvoorwaarden. Empirische onderzoeken die er zijn op het gebied van smart surveillance richten zich met name op de percepties, ervaringen en acceptatie door burgers en in mindere mate de politiemedewerkers zelf. Empirisch onderzoek naar de opbrengsten in termen van een veiligere samenleving zijn schaars.

In de bestudeerde literatuur is privacy het belangrijkste aandachtspunt. Die kan namelijk bij alle vormen van smart surveillance in het geding zijn en zowel zichtbaar als onzichtbaar worden aangetast. Smart surveillance veronderstelt namelijk het op grote schaal verzamelen en analyseren van privacygevoelige data en beeldmateriaal. Privacy wordt vaak benaderd als het prijskaartje van veiligheid. Waar sommige auteurs bij smart surveillance wijzen op een spanningsveld of afweging tussen persoonlijke privacy en publieke veiligheid (Zeng e.a., 2019) lieten Pavone & Esposti (2012) op basis van empirisch onderzoek zien dat dit genuanceerder ligt. Hun analyse liet zien dat geen van de respondenten privacy wilde inruilen voor veiligheid. Dergelijke empirische onderzoeken zijn van belang om een inhoudelijke en beredeneerde afweging te kunnen maken ten aanzien van de voordelen en risico's van smart surveillance waar de discussie nu nog vooral op aannames gebaseerd lijkt te zijn.

In veel artikelen wordt daarom gepleit voor grondige empirische studies naar de daadwerkelijke impact van toepassingen die onder smart surveillance worden geschaard (Fallik e.a., 2020; Goetschel & Peha, 2017; Demir e.a., 2020). Dit betreft de impact op zowel de burgers die object van smart surveillance zijn, als politiemensen die met behulp van smart surveillance toepassingen de handel en wandel van burgers observeren en registreren.

Hoofdstuk 5: Automated policing

5.1 Inleiding

Zoals Kernaghan (2014) reeds in 2014 constateerde, is de inzet van robots en gerobotiseerde systemen in de samenleving inmiddels geen 'science fiction' meer. In Nederland werd in dat kader in 2015 reeds gesproken over de robotsamenleving (Van Est & De Kool red., 2015; Went, Kremer & Knotterus, 2015). Steeds meer organisaties binnen het veiligheidsdomein, waaronder de politie en het leger, zetten robots in bij de uitvoering van hun taken (Gettinger & Michel, 2016). Ook in 'slimme steden' (smart cities) zijn gerobotiseerde en geautomatiseerde systemen in opkomst. Desondanks hebben publicaties over smart cities vaak nog een speculatieve strekking (Macrorie, Marvin & While 2021). Dat geldt ook voor het politiedomein. Doorgaans is de mate van intelligentie en autonomie van robots en gerobotiseerde systemen die door politieorganisaties worden ingezet, nog relatief gering.

In dit hoofdstuk worden de internationale ervaringen van de politie met gerobotiseerde systemen en politierobots belicht. De toepassing van robots en gerobotiseerde systemen door politieorganisaties wordt in de internationale literatuur ook wel automated policing of robotic policing genoemd (Joh, 2018b; Wanebo, 2018; Jackson, 2020). In dit hoofdstuk zal de (minder beladen) term automated policing worden gehanteerd. In hoofdstuk 2 is AI gedefinieerd als 'systems that display intelligent behavior by analyzing their environment and taking actions – with some degree of autonomy – to achieve specific goals.' Wanneer we deze definitie koppelen aan gerobotiseerde systemen en politierobots die de politie gebruikt, dan moeten daar de toepassingen onder worden geschaard die intelligent opereren op basis van een zekere autonomie. De mate van autonomie kan variëren. Naarmate de intelligentie toeneemt, stijgt het potentieel om autonoom te handelen of geautomatiseerde beslissingen te nemen. In dit hoofdstuk worden gerobotiseerde systemen en politierobots op het brede spectrum belicht.

Beide toepassingsvarianten leveren namelijk waardevolle en nuttige lessen en inzichten op. Belangrijk is om te benadrukken dat er tussen deze twee uitersten ook veel tussenvarianten te onderscheiden zijn. Het zijn voornamelijk de tussenvarianten waar momenteel volop mee wordt geëxperimenteerd in de samenleving en dus ook bij de politie.

In paragraaf 5.2 worden politierobots en gerobotiseerde systemen nader gedefinieerd. In paragraaf 5.3 worden concrete toepassingen in het buitenland beschreven. In paragraaf 5.4 wordt aandacht besteed aan de beoogde kansen en in paragraaf 5.5 passeren de mogelijke risico's de revue. In paragraaf 5.6 zijn de kritische succesfactoren vermeld. In paragraaf 5.7 staan de conclusies en reflecties.

5.2 Politierobots en gerobotiseerde systemen

Robotica is een verzamelterm dat uiteenlopende slimme toepassingen omvat. Het begrip robotica is sterk verweven met het begrip kunstmatige intelligentie, omdat robots bij het uitvoeren van menselijke taken moeten beschikken over intelligentie (Kernaghan, 2014). In de wetenschap bestaat er nog geen eenduidige of gezaghebbende definitie van robots (Lin, Abney & Bekey, 2011). Bij robots wordt vaak in eerste instantie gedacht aan apparaten die uiterlijk een beetje op mensen lijken. In dit onderzoek zal echter een brede definitie van robots worden gehanteerd en wordt een robot opgevat als 'any machine that can collect information, process it, and use it to act upon the world' (Joh, 2016). Op basis van deze definitie kunnen ook drones onder robots worden geschaard die zijn uitgerust met camera's en sensoren om specifieke publieke plekken op afstand vanuit de lucht te monitoren (Calo,

2020). In dat kader worden dergelijke drones ook wel luchtrobots genoemd (Royakkers, Daemen & Van Est, 2012). Datzelfde geldt voor onbemande voertuigen die door het leger worden gebruikt om verdachte voorwerpen te inspecteren of explosieven op afstand onschadelijk te maken (Gettinger & Michel, 2016). Doorgaans worden robots ingezet om taken te vervullen die 'dull, dirty or dangerous' zijn (Lin, Abney & Bekey, 2011). Dit betreft dus saaie routinetaken, vieze taken of gevaarlijke taken.

Bij automated policing kunnen politietaken met of zonder tussenkomst van politieagenten worden uitgevoerd (Wanebo, 2018). Bij politietaken die 'op afstand' door politierobots worden uitgevoerd, liggen de autonomie, regie en controle bij agenten. De agenten bedienen namelijk de apparaten en beslissen op basis van de verzamelde gegevens om al dan niet tot actie over te gaan. Agenten zijn dus wanneer ze apparaten op afstand besturen letterlijk 'in control'.

Politietaken kunnen ook worden uitgevoerd zonder tussenkomst van politieprofessionals. Bij dergelijke toepassingen worden 'beslissingen' genomen door systemen. Volledig autonome politierobots zijn momenteel nog toekomstmuziek.

In de literatuur worden verschillende typen robots en gerobotiseerde systemen onderscheiden (Theodoridis & Hu, 2012; Meghdari & Alemi, 2018). De eerste betreft 'sociale' robots die communiceren met burgers. Daarbij kan gedacht worden aan dienstverleningsrobots of balierobots.[11] In de internationale literatuur zijn ook voorbeelden gevonden van politierobots, namelijk surveillance robots. Dit kunnen apparaten zijn die louter informatie verzamelen, maar ook robots die tot op zekere hoogte interacteren met het publiek. Een tweede categorie betreft robots die de politie ondersteunen bij het uitvoeren van gevaarlijke taken, bijvoorbeeld het betreden van gebouwen. Dit kunnen apparaten zijn die lijken op robots, maar ook voertuigen. De derde categorie omvat al dan niet autonome robots die verdachte personen kunnen uitschakelen of doden. Dit worden ook wel bomrobots of killer robots genoemd.[12] Die (kunnen) worden ingezet om mensen uit te schakelen, op afstand bestuurbare voertuigen die politiemensen ondersteunen tijdens operationele handelingen, bijvoorbeeld het betreden van gebouwen, en tot slot gerobotiseerde systemen, die onder meer kunnen worden ingezet om verhoren af te nemen.

Deze verschillende typen robots en gerobotiseerde systemen worden in de volgende paragraaf nader belicht aan de hand van concrete toepassingen in het buitenland.

5.3 Concrete toepassingen in het buitenland

In deze paragraaf worden concrete toepassingen op het gebied van automated policing belicht.

5.3.1 Surveillance robots

De politierobot Xavier in Singapore

Een voorbeeld van een surveillance robot is te vinden in Singapore, waar onlangs een experiment is gestart met de inzet van de politierobot Xavier (Sheema e.a., 2022). Deze politierobot werd ontwikkeld door Singapore's Home Team Science and Technology Agency (HTX). Deze organisatie heeft als taak om technologie te ontwikkelen ten behoeve van de nationale en publieke veiligheid.[13] Een belangrijk

[11] https://www.binnenlandsbestuur.nl/digitaal/achtergrond/achtergrond/liever-een-mens-dan-een-robot.14293964.lynkx

[12] https://www.volkskrant.nl/nieuws-achtergrond/discussie-over-inzet-bomrobot-in-dallas-grens-tussen-politie-en-leger-vervaagt~b31e2d5e/

[13] https://www.popsci.com/technology/xavier-robots-singapores-surveillance-machines/, geraadpleegd op 11 januari 2022.

motief is het realiseren van kostenbesparingen. De autonome robot Xavier gaat toezien op (kleine) overtredingen, waaronder illegale straatverkoop, roken op verboden plekken, verkeerd geparkeerde fietsen, rijden op fietspaden en samenscholingen van meer dan vijf personen. Om ervoor te zorgen dat Xavier zijn werk goed kan doen en zich autonoom kan verplaatsen, is deze robot uitgerust met diverse technische hulpmiddelen, waaronder 360-graden camera's, infrarood sensoren voor nachtzicht en LED-verlichting. De camerabeelden worden naar een commando- en controlecentrum verzonden en met behulp van AI geanalyseerd.[14] In tegenstelling tot echte politieagenten treedt de robot zelf niet handhavend op. Xavier signaleert als surveillance robot overtredingen. De mensen in het commando- en controlecentrum beslissen op basis van de geregistreerde camerabeelden welke passende menselijke interventies noodzakelijk zijn. Xavier is wel voorzien van een groot tabletscherm aan de voorkant waarop een meldings- of waarschuwingsbericht staat voor mensen die (vermoedelijk) de wet overtreden. Het doel van dit bericht is "to educate the public and deter such behaviors".[15] In dat kader is Xavier eerder een helpend handje van de politie, dan een gerobotiseerde politieagent. Xavier heeft geen bevoegdheid om handhavend op te treden. Xavier kan ook in beperkte mate communiceren met burgers door middel van het afspelen van 'pre-recorded messages'. Het is nog te vroeg om lessen te trekken uit de ervaringen die momenteel met Xavier worden opgedaan. Xavier is een redelijk intelligent systeem, maar niet autonoom. Xavier voedt namelijk op afstand de politieorganisatie met gegevens en treedt zelf niet als handelende politieagent op.

Digidogs in New York

In 2020 zette de New York City Police Department (NYPD) zogeheten 'digidogs' in voor verschillende toepassingen (Reid & Gilbert, 2022). Om sociale en historische reden gingen de digidogs reeds in 2021 met pensioen.[16] Een reden is dat het publiek negatief reageerde op digidogs. Het design speelde daarbij mogelijk een rol, Digidogs hadden bijvoorbeeld geen 'gezicht' en hadden als gevolg daarvan geen herkenbare 'menselijke' kenmerken. Verder werd de manier waarop digidogs zicht voortbewogen ervaren als 'creepy'. Ook de specifieke situatie waarin digidogs werden ingezet speelden een rol bij de negatieve houding van burgers ten aanzien van digidogs. Zo werden digidogs ingezet in wijken met sociale woningbouw waarbij reeds sprake was een 'power imbalance' die verder werd vergroot door de inzet van technologie. Wanneer de digidogs in andere situaties zouden zijn ingezet, bijvoorbeeld situaties waarbij burgers geholpen moesten worden, bijvoorbeeld mensen redden uit brandende huizen, dan zou het publiek wellicht anders hebben gereageerd op digidogs. Ook de timing was ongelukkig in het licht van de zorgen van het publiek over de inzet en houding van de politie tegenover minderheden en de zorgen over militarisering van de Amerikaanse politie, waarbij burgers als 'vijanden' van de politie werden benaderd. Net als Xavier hebben digidogs een zekere mate van intelligentie, maar was van autonoom handelen geen sprake.

5.3.2 Ondersteunende operationele politierobots

Surveillance robots worden ingezet om te surveilleren in het publieke domein. Er zijn ook specifieke politierobots die kunnen worden ingezet om politieagenten of politieteams te ondersteunen tijdens (gevaarlijke) operaties. In de Verenigde Staten hebben verschillende Special Weapons and Tactics (SWAT) teams van de politie getraind met operationele politierobots die directe ondersteuning bieden tijdens operaties van deze eenheden (Bethel e.a., 2012). SWAT teams van de politie zijn getraind en

[14] https://www.dutchcowboys.nl/technology/eerste-robocops-gaan-patrouilleren-in-singapore
[15] https://www.popsci.com/technology/xavier-robots-singapores-surveillance-machines/, geraadpleegd op 11 januari 2022.
[16] https://www.scientificamerican.com/article/the-nypds-robot-dog-was-a-really-bad-idea-heres-what-went-wrong/, geraadpleegd op 11 januari 2022.

speciaal opgeleid voor gevaarlijke operaties. Dit betreft onder meer het arresteren van (vuurwapen)gevaarlijke verdachten, het uitschakelen van bewapende daders of het beëindigen van gijzelingen. Bij dergelijke gevaarlijke situaties kunnen gerobotiseerde apparaten nuttig zijn, bijvoorbeeld om waardevolle inlichtingen te verzamelen op basis waarvan SWAT teams interventies kunnen plegen. Gerobotiseerde systemen kunnen bijvoorbeeld als eerste een gebouw betreden en fungeren als oren en ogen van SWAT teams, alvorens de speciaal getrainde politieagenten zelf het gebouw betreden. Het voordeel van de ingezette robots is dat deze klein zijn, uitstekend manoeuvreerbaar en op afstand bestuurd kunnen worden. Ze kunnen dus moeilijk bereikbare of gevaarlijke plaatsen betreden en informatie verzamelen over de situatie ter plekke via camera's of sensoren. Obstakels in deze ruimtes, bijvoorbeeld trappen, dozen en andere voorwerpen kunnen wel voor problemen zorgen. De toegevoegde waarde van robots kan per operatie verschillen. Bij operaties waarbij snelheid is vereist, kan een robot achterop raken en een obstakel worden in plaats van een hulpmiddel. Bij 'langzame' operaties, bijvoorbeeld de benadering en betreding van een pand, kan een robot een nuttig 'lid' van het SWAT-team zijn. Met licht kunnen ze daders verblinden en met geluid kunnen ze daders intimideren. Op deze manier kunnen robots behulpzaam zijn bij het uitschakelen van terroristen. Uit de trainingen met robots is gebleken dat SWAT teams vooral een rol zien weggelegd voor robots in de 'punt van de aanval', dus als schakel tussen de verdachten die ingerekend of uitgeschakeld moeten worden en de leden van het SWAT team. Zij bieden in deze rol extra bescherming aan de leden van het team. De geluiden van gerobotiseerde systemen kunnen de verplaatsingen van leden van SWAT teams ook maskeren en ook dat werd ervaren als een belangrijk voordeel.

Op afstand bestuurbare robots worden ook wel 'telerobots' of 'telepresence robots' genoemd (Prabakar & Kim, 2013). Ze kunnen worden bediend door gezonde politieagenten, maar ook door agenten (of militairen) die als gevolg van handicaps of lichamelijke oorlogsletsels niet meer hun oude taken op straat (of in oorlogsgebieden) kunnen vervullen (Prabakar & Kim, 2013). Het bedienen van telerobots zorgt ervoor dat zij hun kennis en ervaring toch nog in kunnen zetten in de samenleving. Op afstand bestuurbare robots zijn minder intelligent dan surveillance robots, omdat ze op afstand worden bestuurd. Ze zijn evenmin autonoom omdat ze letterlijk worden bediend en aangestuurd door politieagenten.

5.3.3 Op afstand bestuurbare bomrobots

Op afstand bestuurbare bomrobots zijn ondersteunende robots die worden ingezet met een specifiek doel, namelijk het uitschakelen van gevaarlijke personen die een acute bedreiging vormen voor politieagenten of omstanders in de publieke ruimte. Daarom worden bomrobots in dit hoofdstuk separaat besproken. In de Verenigde Staten werd ruim vijf jaar geleden voor het eerst ervaring opgedaan met 'bomrobots' in Dallas (Wanebo, 2018; Jackson, 2020). In de ochtend van 8 juli 2016 zette de politie in Dallas een remotely controlled verhicle (RCV) met een explosief in om een gewapende dader (de oorlogsveteraan Micah Xavier Johnson) die zich had verschanst in de hal van een gebouw, onschadelijk te maken die de avond daarvoor vijf politieagenten had gedood en meerdere mensen had verwond tijdens een vreedzame demonstratie. Deze demonstratie vond plaats naar aanleiding van de dood van twee zwarte mannen. De dader van de schietpartij in Dallas had een militaire achtergrond. Hij hanteerde de militaire strategie van 'shot and move' waardoor de politie in eerste instantie dacht aan meerdere daders (Jackson, 2020). Na de schietpartij had hij zich verschanst en dreigde meer politiemensen te doden. Onderhandelingen leverden niets op. De dader vertelde dat hij meerdere bommen in het centrum van Dallas had geplaatst. Hij gaf ook aan dat het doel van zijn actie was geweest om zo veel mogelijk mensen te doden. Daarna werd een op afstand bestuurd voertuig met een explosief ingezet die de dader ter plekke doodde. Dit was voor het eerst in de

Amerikaanse geschiedenis dat de politie een dader op afstand doodde door middel van een 'bomrobot'. In Dallas betrof dit een voertuig die op afstand te besturen was (een zogeheten 'Remotely Controlled Vehicle', afgekort RCV), die voorzien was van een explosief (Wanebo, 2018). Wanebo (2018) spreekt in dat kader van 'remote policing'. Deze gebeurtenis riep verschillende reacties op. De dader werd uitgeschakeld zodat hij niet meer mensen kon doden. Tegelijkertijd werden kritische vraagtekens geplaatst bij de 'militarisering' van de politie in de Verenigde Staten. Een relevant detail is dat hier sprake was van een geïmproviseerde toepassing. Het op afstand bestuurbare apparaat was namelijk niet ontworpen om mensen te doden, maar om bommen op afstand onschadelijk te maken (Joh, 2016). Ook was het apparaat destijds niet voorzien van kunstmatige intelligentie en handelde het voertuig evenmin autonoom. De verwachting is dat dit in de toekomst wel het geval kan zijn. Een belangrijke vraag bij autonome robots is wie verantwoordelijk is bij de toepassing van (dodelijk) geweld door deze apparaten (Asaro, 2016). Die vraag is bij de politie urgenter dan bij het leger, omdat het gebruik van (dodelijk) geweld door de politie minder wordt geaccepteerd door de samenleving dan geweld door het leger tegen vijanden van de staat (Joh, 2016). De casus in Dallas versterkt verder de vrees van 'militarisering' bij de politie in de Verenigde Staten, waarbij burgers worden benaderd als vijanden van de politie (Doherty, 2016). Op afstand bedienbare bomrobots zijn in beperkte mate intelligent en evenmin autonoom. Het zijn uiteindelijk politieagenten die besluiten om bomrobots al dan niet gericht in te zetten bij het uitschakelen van personen. Dat is geen eenvoudige beslissing, omdat er wordt besloten over leven en dood. Dat verklaart vermoedelijk het feit dat er na Dallas geen beroep meer werd gedaan op bomrobots. In Nederland riep de inzet van de bomrobot in Dallas vooral kritische reacties op, dus de inzet van bomrobots in ons land is tot op heden een ondenkbaar fenomeen en onrealistisch scenario.[17]

Naast bomrobots zijn er ook zogeheten 'killer drones' die vooralsnog alleen worden ingezet door krijgsmachten. Een recent voorbeeld is de in Turkije ontwikkelde Bayraktar TB2 drone die door het Oekraïense leger werd ingezet om Russische militaire voertuigen te vernietigen.[18] Deze drone, die kan worden uitgerust met lasergeleide bommen, wordt op afstand aangestuurd via een satellietverbinding en kan op grote afstand worden ingezet om vijandelijke doelen te bestoken. De drone kan autonoom opstijgen en landen. Ook in Nederland gaan geluiden op om killer drones aan te schaffen voor de Nederlandse krijgsmacht.[19]

5.3.4 Autonome killer robots

Een stap verder dan op afstand bestuurbare bomrobots gaan zogeheten 'killer robots' (Karppi, Böhlen & Granata, 2018; Wood, 2020). Killer robots zijn autonome wapensystemen die mensen kunnen selecteren en uitschakelen zonder menselijke interventies (Karppi, Böhlen & Granata, 2018). Deze systemen worden ook wel 'Lethal Autonomous Weapon Systems' (LAWS) genoemd (Wood, 2020). Dergelijke systemen worden (nog) niet door de politie ingezet, maar wel door het leger. In het licht van de voortschrijdende militarisering van de politie in de Verenigde Staten, kan niet worden uitgesloten dat er op enig moment ook politiekorpsen zijn die killer robots gaan inzetten, ook al roept

[17] https://www.ad.nl/dossier-schietpartij-dallas/inzet-bomrobot-in-dallas-roept-ook-vragen-op~a8ce6bdf/; https://www.volkskrant.nl/nieuws-achtergrond/discussie-over-inzet-bomrobot-in-dallas-grens-tussen-politie-en-leger-vervaagt~b31e2d5e/; https://www.trouw.nl/nieuws/inzet-bomrobot-roept-ook-vragen-op~bc859376/

[18] https://www.dronewatch.nl/2022/02/28/special-zo-worden-civiele-en-militaire-drones-ingezet-voor-de-oorlog-in-oekraine/

[19] https://dvhn.nl/extra/Kamermeerderheid-wil-killerdrones.-Defensie-moet-bommen-en-raketten-onder-dronevliegtuigen-hangen-27609354.html

de inzet daarvan serieuze morele en ethische bezwaren op. De kans dat killer robots op enig moment in Nederland worden ingezet, is vrij klein. In tegenstelling tot de Verenigde Staten zijn de betrekkingen in Nederland tussen politieagenten en burgers doorgaans gemoedelijk van aard. Daarnaast is de militarisering van de politie in hoge mate een Amerikaans fenomeen.

Terroristen zullen zich niets aantrekken van morele en ethische overwegingen en kunnen op enig moment ook killer robots gaan inzetten. Zij hoeven zichzelf niet op te blazen als een zelfmoordrobot ook hun werk kan doen (Sharky in: Royakkers & Van Est, 2015). Daar staat tegenover dat een zelfmoordaanslag door bepaalde terroristen uit religieuze overtuigingen kan worden benaderd als een 'goede' daad die wordt 'beloond' in het hiernamaals.

In tegenstelling tot op afstand bestuurbare bomrobots zijn autonome killer robots intelligent. Ze moeten namelijk in staat zijn om veel gegevens te analyseren op basis waarvan kan worden bepaald dat een bepaald persoon of konvooi een acute bedreiging vormen. Op basis daarvan kunnen killer robots zelfstandig 'besluiten' om tot actie over te gaan. In het Amerikaanse leger worden killer robots reeds ingezet in oorlogsgebieden. Bij politieorganisaties buiten de Verenigde Staten zijn tot op heden geen autonome killer robots ingezet, maar het is natuurlijk niet ondenkbaar dat op enig moment de discussie oplaait om killer robots in te zetten, bijvoorbeeld na incidenten die een grote impact hebben op de samenleving, zoals een terroristische aanslag of een dodelijke schietpartij waarbij veel slachtoffers zijn te betreuren. Dan kunnen emotionele overwegingen eventuele rationele en ethische overwegingen verdringen.

5.4 Beoogde kansen

Op basis van de bestudeerde literatuur kunnen verschillende (beoogde) voordelen van gerobotiseerde systemen en politierobots worden benoemd.

Veiligheid in samenleving verhogen

Robots en gerobotiseerde systemen kunnen een belangrijke bijdrage leveren aan het veiliger maken van een samenleving. Dat gebeurt wanneer deze systemen een bijdrage leveren aan 'lower crime rates' (Joh, 2019). Het veiliger maken van de samenleving door criminaliteit effectief aan te pakken, is een gedeelde doelstelling van politieorganisaties wereldwijd. Politierobots kunnen fungeren als extra ogen en oren van de politie in de publieke ruimte. Surveillance robots kunnen de publieke ruimte efficiënt en effectief monitoren en observeren en daarmee de openbare orde handhaven. Datzelfde geldt voor onbemande voertuigen, de unmanned aerial vehicles (UAVs), die zijn voorzien van camera's en sensoren (Acevedo e.a., 2014). Dit kan resulteren in lagere criminaliteitscijfers (Joh, 2019). Tegelijkertijd kunnen surveillance robots een preventieve werking hebben, omdat mensen weten dat hun gedragingen in de openbare ruimte worden gemonitord en geregistreerd. Dit kan resulteren in minder (onnodig) geweld (Joh, 2019).

Meer efficiency en kostenbesparingen

De inzet van robots en gerobotiseerde systemen kan het politiewerk efficiënter en goedkoper maken. Het realiseren van meer efficiency en kostenbesparingen zijn daarom belangrijke motieven om deze systemen in te zetten (Theodoridis & Hu, 2012; Royakkers & Van Est, 2015; Joh, 2019). Dit motief speelt een belangrijke rol bij surveillance robots.

Politiewerk veiliger en uitdagender maken

Robots kunnen het werk voor politieagenten veiliger maken (Theodoridis & Hu, 2012; Joh, 2016). Robots kunnen bijvoorbeeld als eerste gevaarlijke plekken betreden, zodat politieagenten geen onnodig gevaar lopen (Royakkers & Van Est, 2015). Dit motief speelt voornamelijk een rol bij robots die ingezet worden bij operationele activiteiten van (speciale) politie eenheden of bij bomrobots die gevaarlijke mensen op afstand moeten uitschakelen. Politierobots kunnen op die manier gevaarlijke politietaken overnemen (Royakkers & Van Est, 2015). Dergelijke robots zijn vaak oorspronkelijk ontwikkeld voor militaire doeleinden. Robots in het leger worden vaak ingezet om de drie D-taken uit te voeren, namelijk werkzaamheden die dull, dirty en dangerous zijn (Royakkers & Van Est, 2015: Lin, Abney & Bekey, 2011). Politierobots en gerobotiseerde systemen kunnen ook saaie en routinematige handelingen overnemen van politiemedewerkers (Royakkers & Van Est, 2015). Op deze manier kunnen ze agenten ontlasten en ontzorgen. Vanuit deze invalshoek gaan politietaken niet verdwijnen, maar wel veranderen, omdat robots en gerobotiseerde systemen een deel van de surveillance en administratieve taken gaan overnemen (Joh, 2018b).

Minder fouten en hogere betrouwbaarheid bij het politiewerk

Gerobotiseerde systemen kunnen minder fouten maken dan mensen (Royakkers & Van Est, 2015). Bij het afleggen van verhoren kunnen bijvoorbeeld vooroordelen of 'biases' voorkomen worden. Dit kan resulteren in verklaringen van daders en slachtoffers die betrouwbaarder zijn. Dit (vermeende) voordeel treedt uiteraard alleen op wanneer er in de historische data op basis waarvan het gerobotiseerde systeem leert, geen biases zitten. Ook de context speelt een rol. In bepaalde situaties zullen burgers hun confronterende en traumatiserende ervaringen wellicht opener delen in een virtuele setting, dan in een offline omgeving. Dat kan per persoon en per vergrijp verschillen.

5.5 Mogelijke risico's

Op basis van de bestudeerde literatuur kunnen ook enkele (mogelijke) risico's worden benoemd.

Aantasting van privacy

Robots die zijn voorzien van camera's en sensoren kunnen beelden en geluiden vastleggen en daarmee de privacy van burgers aantasten (Lin, Abney & Bekey, 2011; Royakkers & Van Est, 2015; Reid, 2017; Van Est e.a., 2017; Calo, 2020). Ze kunnen zichtbaar zijn voor burgers en daarmee expliciet hun privacy aantasten (door middel van robots die zichtbaar surveilleren in de publieke ruimte), maar dit ook heimelijk doen (bijvoorbeeld door middel van drones die burgers onzichtbaar vanuit het luchtruim op afstand volgen). De privacy van burgers kan dus bewust, maar ook onbewust worden aangetast door robots en gerobotiseerde systemen van de politie. De vraag is ook wie er toegang heeft tot de verzamelde data en waar en hoe lang deze data wordt bewaard.

Hacking

Robots en gerobotiseerde systemen kunnen door derden worden gehacked (Lin, Abney & Bekey, 2011; Calo, 2020). Als gevolg daarvan kunnen ze onbedoeld onwenselijke handelingen gaan verrichten. Dit kan resulteren in gevaarlijke situaties, zekere wanneer dit bomrobots betreft of systemen die de politie ondersteunen tijdens operationele werkzaamheden. Ze kunnen ook worden geïnfecteerd met virussen (Royakkers & Van Est, 2015; Sumantri, 2019).

Programmeerfouten

Het maken van minder fouten is zojuist benoemd als voordeel. Aan de andere kant kunnen gerobotiseerde systemen ook fouten maken, bijvoorbeeld als gevolg van programmeerfouten in de software (Lin, Abney & Bekey, 2011; Meghdari & Alemi, 2018). Daarnaast kunnen in AI impliciete biases ten grondslag liggen en die kunnen impliciet doorwerken bij de gehanteerde algoritmes. Programmeerfouten kunnen ook grote gevolgen hebben voor burgers. De vraag is wie uiteindelijk verantwoordelijk is voor de gevolgen van (programmeer)fouten die systemen maken: de ontwikkelaars van deze systemen, de gebruikers van deze systemen of de autonome systemen zelf? Het is nu nog toekomstmuziek, maar zeker niet ondenkbaar dat politierobots zich op enig moment moeten verantwoorden bij rechters nadat ze fatale fouten hebben gemaakt. Mede in dat kader worden veiligheidstandaarden voor politierobots bepleit (Royakkers & Van Est, 2015).

Technische problemen

Een risico is dat de gerobotiseerde systemen en politierobots onverwacht en onbedoeld uitvallen als gevolg van technische problemen. Dit kunnen technische storingen zijn (bijvoorbeeld kapotte camera's en defecte sensoren), maar ook lege batterijen of accu's. Surveillance robots kunnen dan hun werk niet meer doen. Storingen van gerobotiseerde systemen kunnen de uitvoering van politietaken belemmeren

Ongelijkheid versterken

AI kan biases elimineren, bijvoorbeeld bij het onbevangen verhoren van slachtoffers en verdachten. Tegelijkertijd worden AI-systemen gevoed met historische data waar biases in kunnen zitten. Wanneer dit laatste het geval is, dan kunnen gerobotiseerde systemen de sociale ongelijkheid versterken (Joh, 2016a; Jackson, 2020). Robots kunnen mede als gevolg daarvan ontsporen. Een voorbeeld is de chatbot Tay van Microsoft die op een gegeven moment racistische uitlatingen deed en opriep tot genocide (Joh, 2016).

Militarisering van de politie

Een risico is dat (bewapende) politierobots en bewapende politiesystemen (bijvoorbeeld drones) resulteren in een militarisering van de politie (Jackson, 2020). Dit proces is in de Verenigde Staten begonnen met de vorming van SWAT teams binnen de Amerikaans politie, maar kan een nieuwe impuls krijgen als gevolg van de opkomst van bewapende robots en bewapende politiesystemen. Een risico van militarisering is dat de houding van de politie tegenover burgers kan verharden en dat burgers niet meer worden benaderd als subjecten, maar als vijandelijke objecten die zo nodig uitgeschakeld moeten worden.

Verlies van vaardigheden en competenties

De inzet van politierobots en gerobotiseerde systemen kan resulteren in het verlies van vaardigheden, competenties en kennis bij het uitvoeren van politietaken. In de Engelstalige literatuur wordt in dat kader gewezen op het risico van 'deskilling' (Royakkers & Van Est, 2015; Van Est e.a., 2017; Joh, 2018b; Joh, 2019). Een gevolg van de opkomst van navigatiesystemen is dat er steeds minder een beroep wordt gedaan op ons eigen navigatievermogen (bijvoorbeeld in de vorm van kaartlezen). Dit kan ervoor zorgen dat mensen dergelijke vaardigheden geleidelijk verleren. Datzelfde geldt voor politietaken die worden overgenomen door robots en gerobotiseerde systemen. Bij surveillance robots verdwijnt er bijvoorbeeld heel veel data en beeldmateriaal in digitale systemen waar surveillerende agenten mogelijkerwijs ter plekke niet direct over kunnen beschikken.

Politiemensen vervangen

Kansen doen zich voor wanneer robots supplementair zijn en politiemedewerkers aanvullen en ondersteunen. Desondanks worden politierobots en gerobotiseerde systemen ook als bedreigend ervaren vanuit de angst dat ze mensen gaan vervangen en hun functies gaan 'overnemen'. Die angst is mede gebaseerd op ontwikkelingen in andere sectoren en domeinen, bijvoorbeeld de logistiek (Joh, 2019). De menselijke kant van het politiewerk blijft wel van groot belang. Wanneer de menselijke dimensie wordt veronachtzaamd, dan kan dehumanisering optreden. Dit brengt ons bij het volgende risico.

Dehumanisering

De inzet van robots en gerobotiseerde systemen kan (onbedoeld) resulteren in de dehumanisering van mensen (Royakkers & Van Est, 2015). Zeker op het gebied van dienstverlening en communicatie kunnen gerobotiseerde systemen de 'warme' menselijke communicatie weliswaar verrijken, maar doorgaans niet vervangen. Robots en gerobotiseerde systemen kunnen een psychologische afstand tussen de politieorganisatie en burgers creëren en dat kan weer resulteren in dehumanisering van politiepraktijken (Jackson, 2020). Tegen die achtergrond wordt in de literatuur ook gepleit voor het recht op betekenisvol menselijk contact ('meaningful human contact') (Van Est e.a., 2017).

5.6 Kritische succesfactoren

Bij het effectief inzetten van robots en gerobotiseerde systemen door de politie moet rekening worden gehouden met verschillende factoren die in de bestudeerde artikelen vaak zijn genoemd.

Wettelijke inkadering

Een dominante kritische succesfactor in de literatuur is de mate waarin juridische overwegingen, bijvoorbeeld op het gebied van privacy, wettelijk zijn ingekaderd. Robots en gerobotiseerde systemen kunnen namelijk zichtbaar en onzichtbaar de privacy van burgers aantasten. In de Verenigde Staten is bijvoorbeeld het vierde amendement van de Amerikaanse grondwet een belangrijk juridisch kader. Dit amendement beoogt burgers te beschermen tegen 'unreasonable government intrusions into private spaces' (Calo, 2020). Een ander relevant juridisch aandachtspunt betreft de vraag wie de eigenaar is van de persoonlijke data die door gerobotiseerde systemen wordt verzameld (Royakkers & Van Est, 2015; Van Est e.a., 2017). Tegen die achtergrond wordt in de literatuur gewezen op het belang van een 'regulatory agenda' (Joh, 2016), 'clear and effective regulatory policies' (Turner, 2018) en een 'legal framework for AI-based systems' (Sumantri, 2019). Bij het benodigde 'legal framework' is samenwerking tussen juristen, AI experts en experts op het domein van robotica noodzakelijk (Sumantri, 2019).

Ethische code

Een tweede belangrijke kritische succesfactor is dat er expliciete aandacht is voor ethische aspecten en dat deze als zodanig een plek hebben gekregen dan wel zijn afgewogen in ethische kaders (Theodoridis & Hu, 2012; Lin e.a. 2014; Royakkers & Van Est, 2015; Meghdari & Alemi, 2018; Turner, 2018). De mate waarin deze kritische succesfactor van toepassing is, wordt mede bepaald door de specifieke inzet van robots en gerobotiseerde systemen. Deze kritische succesfactor is expliciet van toepassing bij robots en gerobotiseerde systemen die worden ingezet om verdachte personen uit te schakelen. De ethische kant betreft niet alleen de wijze waarop mensen robots en gerobotiseerde systemen gebruiken, maar heeft ook betrekking op de (ethische) keuzes die zijn gemaakt tijdens het bouwen van robots en gerobotiseerde systemen (Asaro, 2016). In dat kader wordt in de literatuur

gewezen op het belang van een internationaal debat over sociale en ethische vraagstukken rondom robotica (Royakkers & Van Est, 2015) en een ethische code voor 'human robot interactions' (HRI) (Asaro, 2016). In de Verenigde Staten is er een ethische code die bekend staat als PAPA (privacy, accuracy, intellectual property & access) (Calo, 2020). Kenaghan (2014) heeft bepleit dat de ethische code in ieder geval 'personal moral responsibility, privacy and accountability' omvat (Kernaghan, 2014). Tasioulas (2019) bepleitte een ethisch kader dat de volgende vijf morele 'FIRST' componenten bevat: functionality, inherent significance, rights and responsibilities, side-effects and threats (Tasioulas, 2019).

Maatschappelijke factoren: acceptatie

Een belangrijke kritische succesfactor is dat politierobots en gerobotiseerde systemen worden geaccepteerd door de samenleving (Royakkers & Van Est, 2015). Het draagvlak bij burgers en politieagenten is mede afhankelijk van de mate waarin en de wijze waarop de zojuist genoemde ethische en juridische aspecten zijn ingekaderd. Daarnaast is de mate van acceptatie mede afhankelijk van de context waarin robots en gerobotiseerde systemen worden ingezet. Sociale robots en gerobotiseerde systemen die burgers en politieagenten 'helpen' of 'ondersteunen' zullen bijvoorbeeld doorgaans eerder worden geaccepteerd dan robots die mensen 'heimelijk observeren' of 'uitschakelen'. De mate van acceptatie wordt ook mede bepaald door het vertrouwen van politiemedewerkers en burgers in politierobots en gerobotiseerde systemen (Royakkers & Van Est, 2015; Karpinsky, Long & Bliss, 2017; Turner, 2018). In belangrijke mate wordt dit vertrouwen gevoed (of geschaad) op basis van de directe ervaringen van burgers en politiesystemen met politierobots en gerobotiseerde systemen. Daarom is het belangrijk dat burgers en politieagenten de voor- en nadelen van dergelijke systemen persoonlijk ervaren. Met behulp van proeftuinen kunnen dergelijke ervaringen worden opgedaan en systematisch in kaart worden gebracht.

Technische factoren: betrouwbaarheid

Betrouwbaarheid ('liability') is een belangrijk principe bij de regulering van robots en gerobotiseerde systemen (Royakkers & Van Est, 2015; Van Est e.a., 2017; Sumantri, 2019). Deze betrouwbaarheid heeft duidelijke raakvlakken met veiligheid (Van Est e.a., 2017). Dit betekent dat robots geen onnodige gevaren veroorzaken voor politiemensen of burgers. Een slimme drone kan bijvoorbeeld neerstorten en het is natuurlijk niet de bedoeling dat bomrobots onschuldige burgers uitschakelen.

5.7 Conclusies en reflecties

Afgaand op de in hoofdstuk 2 gehanteerde definitie van AI kan de politie met behulp van automated policing op een intelligente manier de omgeving observeren en gerichte ondersteunende activiteiten uitvoeren om derhalve met een zekere mate van autonomie, specifieke doelen te bereiken. We hebben vastgesteld dat de mate van intelligentie en de mate van autonomie kan variëren. In dit hoofdstuk zijn verschillende toepassingen onderscheiden, namelijk surveillance robots, ondersteunende operationele robots, op afstand bestuurbare bomrobots en autonome killer robots. Op basis van de beschreven voorbeelden zijn verschillende kansen en risico's genoemd die betrekking hebben op de maatschappij (macro), de politieorganisatie (meso) en individuele politieagenten en burgers (micro).

De beoogde kansen hebben betrekking op alle niveaus die in het conceptueel model zijn onderscheiden (macro, meso en micro). Een effectievere aanpak van de criminaliteit met behulp van automated policing komt de hele samenleving ten goede (macro). Het realiseren van kostenbesparingen en efficiënter werken, komt in de eerste plaats de politieorganisatie ten goede

(meso). Het veiliger maken van het politiewerk en het ontlasten van politiemedewerkers door gevaarlijke of saaie routinetaken over te nemen, is in het belang van individuele agenten (micro). De mate waarin de (beoogde) voordelen die zojuist zijn benoemd verzilverd kunnen worden, hangt in belangrijke mate af van de intelligentie van de systemen. Hoe intelligenter de systemen zijn des te groter de bijdrage kan zijn bij het efficiënter en effectiever organiseren en uitvoeren van politietaken, en hoe meer menselijke taken kunnen worden overgenomen. Dit brengt wel een belangrijk dilemma met zich mee, want met de toename van intelligentie en autonomie worden ook de risico's groter, namelijk het verlies van menselijke controle.

De mogelijke risico's hebben betrekking op alle niveaus die in het conceptueel zijn onderscheiden (macro, meso en micro). De mogelijke aantasting van de privacy is een breed maatschappelijk vraagstuk (macro) en kan impact hebben op individuele burgers (micro). De militarisering van de politie in de Verenigde Staten en gedehumaniseerde interacties tussen de politie en burgers hebben maatschappelijke impact (macro), impact op het imago van de politie (meso) en op de interacties tussen individuele burgers en politiemedewerkers (micro). De risico's van het verlies van vaardigheden, competenties en zelfs het verliezen van de eigen baan wanneer robots en gerobotiseerde systemen het takenpakket van politieagenten overnemen en 'mensen vervangen', heeft betrekking op individuele politiemedewerkers (micro). Het risico om een baan te verliezen (micro) kan vanuit mesoniveau anders worden bekeken. Op organisatieniveau (meso) kan het vervangen van mensen door systemen die het politiewerk effectiever en efficiënter kunnen uitvoeren natuurlijk ook voordelen met zich meebrengen. De risico's van hacking, technische problemen en programmeerfouten kunnen de effectiviteit van de politieorganisatie aantasten en bovendien resulteren in imagoschade van de politie (meso). Deze risico's kunnen toenemen naarmate de intelligentie en autonomie van robots en gerobotiseerde systemen toeneemt. Datzelfde geldt voor de impact van de risico's wanneer deze optreden. Het hacken van een autonome en intelligente killer robot kan bijvoorbeeld veel grotere en ernstige gevolgen hebben dan het hacken van een robot die slechts gegevens verzamelt.

Voor wat betreft de kritische succesfactoren is de juridische inkader (ook) bij robotic policing een relevante factor. Vooral de (vermeende) aantasting van de privacy van burgers (microniveau) wordt in dat kader vaak genoemd in de internationale literatuur. Een belangrijke ethische (en maatschappelijke vraag) is hoever de politie moet willen gaan bij het inzetten van automated policing en welke autonome ruimte dergelijke systemen moeten krijgen (mesoniveau). Bij ondersteunende activiteiten die het werk verlichten of minder gevaarlijk maken, is de acceptatie doorgaans hoger dan bij taken die 'ongevraagd' worden overgenomen. Om die reden is het van groot belang om de werkvloer, in dit geval politiemedewerkers, vroegtijdig en proactief te betrekken bij de ontwikkeling van gerobotiseerde toepassingen (Wisskirchen e.a., 2017). Het belang van breed maatschappelijk draagvlak heeft betrekking op het macroperspectief. Tegelijkertijd is het belangrijk dat politierobots en gerobotiseerde systemen worden geaccepteerd op microniveau door politieagenten die met politierobots en gerobotiseerde systemen moeten (samen)werken. Technische factoren hebben onder meer betrekking op maatregelen om systemen te beveiligen tegen hacking, programmeerfouten te voorkomen en om de betrouwbaarheid van systemen te verhogen (mesoniveau). Als gevolg van hacking kunnen politiegegevens in handen van derden belanden en dat kan implicaties hebben voor individuen (microniveau).

De mate waarin rekening wordt gehouden met de kritische succesfactoren is mede afhankelijk van de context, de specifieke inzet en de mate waarin de politierobots en gerobotiseerde systemen intelligent en autonoom zijn. Reid (2017) bepleit een samenwerking tussen juristen en technici om de mate van autonomie van robots en controle van mensen op gerobotiseerde systemen te bepalen. Hoe

intelligenter en autonomer de toepassingen zijn, hoe groter de impact van deze toepassingen voor de maatschappij (macro), de politieorganisatie (meso), de individuele burgers die met deze toepassingen worden geconfronteerd en de politieagenten die met dergelijke systemen (samen)werken. Hoe autonomer de ruimte van deze systemen is, hoe belangrijker het wordt om juridische, ethische, maatschappelijke en technische factoren, randvoorwaarden en eisen goed en zorgvuldig in te kaderen. De maatschappelijke en individuele impact van robots en gerobotiseerde systemen kan namelijk groot zijn en zal naar verwachting groter worden. In dat kader is het misschien wel een geruststellende gedachte dat intelligente en autonome robots en gerobotiseerde toepassingen bij de politie nog geen gemeengoed zijn, zodat er nog tijd is om de bedoelde en onbedoelde consequenties goed te doordenken.

6 Overige toepassingen en reflecties

6.1 Inleiding

In dit hoofdstuk worden de internationale ervaringen van de politie met de overige toepassingen op het gebied van AI belicht. Dit betreft toepassingen die niet eenduidig te plaatsen zijn binnen de drie onderscheiden clusters in dit onderzoek. Deze toepassingen worden beschreven in paragraaf 6.2. In paragraaf 6.3 worden de beoogde kansen beschreven en in paragraaf 6.4 de mogelijke risico's. In paragraaf 6.5 volgt een opsomming van kritische succesfactoren. In paragraaf 6.6 worden de reflectiepunten van (buitenlandse) politieonderzoekers en -experts belicht die tijdens de uitvoering van deze internationale literatuurstudie digitaal werden geconsulteerd. In paragraaf 6.7 staan de conclusies.

6.2 Concrete toepassingen in het buitenland

AI tijdens het verhoorproces

Noriega (2020) heeft in een artikel aandacht besteed aan het potentieel van AI tijdens het afnemen van verhoren door de politie. Hierbij kan onder ander worden gedacht aan slimme software die in staat is om zowel visuele als verbale emotionele veranderingen realtime te analyseren. De gedachte hierachter is dat AI ervoor kan zorgen dat verdachten onbevangen en zonder vooroordelen ('biases') verhoord kunnen worden. Daarnaast wordt het risico dat verklaringen onder druk worden afgelegd, verminderd of helemaal weggenomen. Het risico van valse verklaringen wordt hiermee verkleind. Bij verhoren die worden afgenomen door mensen ligt namelijk het risico op de loer dat racistische vooroordelen of 'gender bias' een rol spelen en dat het verhoorproces als gevolg daarvan niet onbevangen verloopt. Hier is nog geen empirisch onderzoek naar gedaan.

Verhoorrobots voor kinderen

Gerobotiseerde politiesystemen kunnen worden ingezet om kinderen te verhoren (Kyriakidou e.a., 2013). Daarbij kan gebruik worden gemaakt van computers of Closed Circuit Television (CCTV). Een belangrijk motief is dat kinderen 'cute' robots mogelijk eerder accepteren als gesprekspartner dan volwassen mensen. Een tweede motief is dat kinderen tijdens verhoren mogelijk opener zijn over persoonlijke zaken, zoals seksueel misbruik of huiselijke problemen wanneer ze vragen door middel van een gerobotiseerd systeem beantwoorden in plaats van dat ze een persoon te woord staan. De verwachting is dat de verklaringen die ze afleggen op het politiebureau als gevolg hiervan accurater en rijker zijn. Een relevant vraagstuk is 'data ownership' (Royakkers & Van Est, 2015; Van Est e.a., 2017). Dit betreft de vraag wie de 'eigenaar' is van persoonsgegevens die op deze manier wordt verzameld: de eigenaar of producent van de robot, de interviewer, de verdachte, het slachtoffer, de politie, advocaten, rechters of de overheid? Ook de veilige opslag van deze data is met het oog op privacy een belangrijk aandachtspunt. Gerobotiseerde verhoorsystemen kunnen in bepaalde opzichten effectiever zijn dan verhoren die door personen worden afgenomen. Daar staan ethische dilemma's tegenover die ook aandacht verdienen. Kyriakidou e.a. (2013) bepleiten daarom voor een protocol, waarin deze belangrijke zaken worden gereguleerd. Gerobotiseerde verhoorsystemen zijn intelligent in de zin dat ze in staat zijn om goede en onbevangen vragen te stellen tijdens het afnemen van verhoren. Ze zijn ook autonoom in de zin dat ze zelf bepalen welke vragen er precies op welk moment worden gesteld. De verhoorverslagen worden uiteindelijk wel beoordeeld en geïnterpreteerd door politiemedewerkers.

Detectie van vuurwapengeluiden

Het detecteren van vuurwapengeluiden is een uitdagende taak voor de politie. Kunstmatige intelligentie wordt gebruikt om op basis van vuurwapengeluiden te kunnen vaststellen welke vuurwapens zijn gebruikt op een plaats delict en welk kaliber ze hebben (Raponi e.a., 2022). In de Verenigde Staten wordt in dat kader ShotSpotter gebruikt. Dit is technologie om met behulp van sensoren vuurwapengeluiden te detecteren.

Detectie van cybercrime

Cybercrime is een groot probleem en heeft veel impact. Sheikha e.a. (n.d.) hebben in een paper aandacht besteed aan de inzet van kunstmatige intelligentie bij het detecteren en voorspellen van cybercrime. AI kan in dat kader worden gebruikt om de enorme datastromen op digitale netwerken te analyseren en vervolgens te bepalen of er digitale criminele delicten zijn of worden gepleegd.

Generieke studies

Gkougkoudis e.a. (2022) hebben in een paper de stand van zaken rondom Intelligence-Led Policing (ILP) bij de Griekse politie verkend. Ze besteden onder meer aandacht aan literatuur over Internet of Things (IoT), Facial Recognition Software, biometrische systemen, robots, ShotSpotter (technologie om vuurwapengeluiden te detecteren met behulp van sensoren), Thermal Imaging, CCTV-systemen en drones (om bijvoorbeeld grenzen te monitoren). Daarnaast besteden ze aandacht aan technologieën die in de Europese Unie worden ingezet, zoals automated fingerprint identification, automated facial recognition technology (FRT), automated border control (ABC).

Gkougkoudis e.a. (2022) concluderen dat er weinig empirisch bewijs voorhanden is om de verwachte kansen en risico's van nieuwe technologieën in de Europese Unie te kunnen vaststellen. Zo is er weinig inzicht in de percepties van burgers ten aanzien van nieuwe technologie die door de politie wordt ingezet. Een relevante vraag is of de inzet van nieuwe technologie invloed heeft op het vertrouwen van burgers in de politie, alsmede de legitimiteit en transparantie van de politie. De onderzoekers bepleiten nader onderzoek op dit terrein. Datzelfde geldt voor ethische vraagstukken die nieuwe technologie oproept. Ze concluderen dat de meeste technologieën op dat vlak zich nog in een onderzoeks- en experimenteerstadium bevinden en dat empirische studies op dat vlak nog niet beschikbaar, maar wel noodzakelijk zijn.

Tao e.a. (2021) hebben een reviewstudie gedaan waarin de toepassing van AI op het gebied van cybersecurity is belicht. Ze besteden aandacht aan concrete technologieën waar AI een rol bij kan spelen, zoals blockchaintechnologie, Internet of Things (IoT) en Intrusion Detective Systems (IDS).

6.3 Beoogde kansen

De beoogde kansen van de overige toepassingen wijken niet fundamenteel af van de voordelen die in de voorgaande hoofdstukken voor het voetlicht zijn gebracht. Dit betreft onder meer het effectiever bestrijden van criminaliteit. Het inzetten van AI tijdens verhoren kan volgens de literatuur resulteren in het onbevangen bevragen van burgers en dit vergroot de kans op betrouwbare aangiften en verkleint de kans op valse verklaringen.

6.4 Mogelijke risico's

De mogelijke risico's van de overige toepassingen wijken niet fundamenteel af van risico's die in de voorgaande hoofdstukken voor het voetlicht zijn gebracht. Bij de overige toepassingen zijn in de literatuur (wederom) als risico's genoemd de aantasting van de privacy van burgers en het gebrek aan transparantie, toezicht en verantwoording. Een risico van het inzetten van een gerobotiseerd systeem om kinderen te verhoren, is dat kinderen een 'fake relationship' met het gerobotiseerde systeem aangaan en het verhoor benaderen als een 'spel' waarin ze hun fantasie de vrije loop kunnen laten. Dit kan resulteren in valse verklaringen ('fake testimonies').

6.5 Kritische succesfactoren

De kritische succesfactoren die in de literatuur bij de overige toepassingen zijn benoemd hebben (wederom) betrekking op ethische principes, acceptatie door en draagvlak bij burgers en juridische waarborgen, zoals het belang van regulering waarbij mensenrechten worden gerespecteerd en discriminatie wordt voorkomen.

6.6 Reflecties van (buitenlandse) politieonderzoekers en -experts

In het voorjaar van 2022 werd een aantal (buitenlandse) politieonderzoekers en -experts digitaal geconsulteerd. De geraadpleegde experts zijn vermeld in bijlage 1. De gebruikte topic list is opgenomen in bijlage 4. Belangrijke doelen van deze digitale consultatieronde waren om nader te reflecteren op AI bij de politie, actuele casuïstiek voor het voetlicht te brengen die (nog) niet is belicht in de internationale literatuur en deze reflecties te benutten bij het formuleren van concrete, beredeneerde en bruikbare aandachtspunten voor de (Nederlandse) politiepraktijk. De belangrijkste reflectiepunten zijn hieronder vermeld.

Ethische kant van AI is een belangrijk thema in het wetenschappelijke discours

De ethische kant van AI is volgens de geconsulteerde experts onderwerp van een levendig debat in de wetenschappelijke literatuur. Deze observatie is in lijn met de bevindingen uit de literatuurstudie, waarin we vaststellen dat de ethische dimensie van AI relatief veel aandacht krijgt. Datzelfde geldt overigens voor de juridische kant van AI.

AI-projecten bij de politie waar (nog) niet over is gepubliceerd

De geconsulteerde experts hebben aangegeven dat er bij de politie in het buitenland de nodige AI-projecten worden uitgevoerd waarover (nog) niet is gepubliceerd in de internationale literatuur. De politie van Edmonton (EPS) in Canada voert bijvoorbeeld momenteel een project uit om kunstmatige intelligentie te gebruiken bij cold cases voor moordzaken. Een ander actueel voorbeeld in de Verenigde Staten is het gebruiken van nieuwe technologie om schoten van vuurwapens ('gunshots') te detecteren. Aan het ontbreken van literatuur kunnen verschillende oorzaken ten grondslag liggen. Een eerste reden is dat er sprake kan zijn van ervaringen die momenteel worden opgedaan door de politie en dus nog te actueel zijn om daarover te publiceren. Artikelen in wetenschappelijke journals zijn doorgaans gebaseerd op onderzoeken die (ruim) voor de publicatiedatum zijn uitgevoerd. Een tweede reden is dat de politie er vaak geen belang bij heeft om ervaringen met AI te delen met de buitenwereld, om criminelen niet in de kaart te spelen.

Onevenwichtige benadering van kansen en risico's

De geraadpleegde experts hebben naar voren gebracht dat AI in de literatuur vaak eenzijdig wordt belicht. Dat geldt zowel voor het belichten van de kansen als de risico's. Deze observatie is herkenbaar wanneer louter wordt ingezoomd op afzonderlijke artikelen. Dan overheerst vaak een positieve (focus op kansen) of negatieve boodschap (focus op bedreigingen). Wanneer meer vanuit een helicopterview naar het grote plaatje wordt gekeken en artikelen naast elkaar worden gelegd, dan kan wel worden vastgesteld dat zowel de kansen als de risico's voldoende aan bod komen en dat het fenomeen AI in de literatuur in zijn totaliteit genuanceerd wordt benaderd. Een blinde vlek die uit de literatuurstudie wel naar voren kwam is dat er relatief weinig aandacht wordt besteed aan de implicaties van AI op microniveau, dus de impact van AI op individuele politieprofessionals en burgers.

Behoefte aan centrale kaders

De experts hebben geconstateerd dat in landen waar de politie decentraal is georganiseerd, bijvoorbeeld de Verenigde Staten, de behoefte aan centrale regulering en kaders groot is. In de Verenigde Staten wordt nu een wildgroei aan lokale initiatieven waargenomen, waarbij centrale regie ontbreekt. Als gevolg daarvan lijkt het erop dat er te weinig wordt geleerd van elkaars ervaringen en iedereen zelf het wiel uitvindt. In Nederland is de situatie anders. Daar is met de vorming van de nationale politie een beweging richting centralisatie in gang gezet.

Dominantie van bedrijven

De geconsulteerde experts hebben gewezen op het feit dat veel AI-technologie in de Verenigde Staten wordt ontwikkeld en geleverd door private bedrijven. Dat geldt dus ook voor veel AI-toepassingen die de politie in het buitenland gebruikt. Voor het bedrijfsleven is AI een grote lucratieve business. Daar kleven volgens de professionals grote risico's aan, bijvoorbeeld structurele afhankelijkheidsrelaties van de politie richting bedrijven. 0ok Nederland is sterk afhankelijk van AI-diensten van Tech giganten (Bakker e.a., 2021). Dit speelt niet bij het CAS, dat door de politie zelf ontwikkeld is.

Samenspel tussen techniek en professionals

De experts hebben geconstateerd dat de relatie tussen (AI)technologie en politieprofessionals gaat veranderen. Daarbij is het nog niet bekend welke kant het opgaat. De kans is aanwezig dat steeds meer (blind) wordt vertrouwd op technologie. Dit kan ten koste gaan van het gewicht dat wordt toegekend aan het gezonde verstand en het professionele oordeel van politiemedewerkers. Volgens de experts is het belangrijk dat er een balans is tussen beide en dat de techniek de mensen niet vervangt, maar aanvult en ondersteunt.

Benaderbaarheid van politiemedewerkers

De experts hebben vastgesteld dat de benaderbaarheid van politiemedewerkers kan variëren. In de Verenigde Staten is die benaderbaarheid niet hoog. De afstanden zijn daar te groot om te voet een rondje te maken. De meeste interacties tussen burgers en politieagenten voltrekken zich daar in het verkeer door middel van patrouilles per auto. Dit creëert een afstand tussen beide. Die afstand kan worden vergroot wanneer er technologie (bijvoorbeeld bodycams) tussen agenten en burgers wordt geplaatst. In Nederland is de afstand tussen (wijk)agenten en burgers doorgaans kleiner. Het is belangrijk om oog te hebben voor het feit dat AI-technologie de afstand tussen politiemedewerkers en burgers kan vergroten.

Vertrouwen in politie varieert

Het vertrouwen van burgers in de politie kan per land verschillen. De politie en burgers in de Verenigde Staten hebben bijvoorbeeld van oudsher een gespannen relatie. Die relatie kan niet los worden gezien van ernstige incidenten in het verleden, zoals de mishandeling van Rodney King in 1991 in Los Angeles en recentere incidenten die hebben geresulteerd in de opkomst van de beweging Black Lives Matter. Technologie kan helpen om die relatie te verbeteren, omdat het optreden van de politie transparanter wordt door bijvoorbeeld het gebruik van bodycams. Nieuwe technologie kan de afstand ook vergroten, zeker wanneer biases en discriminatie doorwerken in AI-toepassingen. In Nederland is het vertrouwen van de politie in burgers relatief hoog. De politie heeft er veel belang bij om dit vertrouwen te handhaven of te vergroten, omdat vertrouwen een belangrijke voorwaarde is om aangifte te doen en gegevens te delen met de politie.

Gebrek aan evaluaties en impactmetingen

De geconsulteerde experts hebben vastgesteld dat er relatief weinig empirisch gefundeerde artikelen over AI bij de politie beschikbaar zijn. Deze observatie is in lijn met onze ervaringen bij de internationale literatuurstudie waarbij we hetzelfde hebben vastgesteld. De experts hebben in dat kader gewezen op het feit dat er weinig tot geen onderzoek is gedaan naar het draagvlak van politiemedewerkers en burgers voor AI-technologie bij de politie. Verder zijn er weinig empirische studies die inzicht bieden in de echte voordelen van nieuwe technologie. Dat is opmerkelijk in het licht van de enorme investeringen van politieorganisaties wereldwijd in nieuwe technologie. Het gebrek aan empirisch gefundeerde artikelen kan volgens de experts verschillende oorzaken hebben. Om te beginnen heeft de politie vaak een doenersmentaliteit. Dat is vaak niet de ideale cultuur om onderzoek te doen naar de adoptie van nieuwe technologie en de opgedane ervaringen grondig te evalueren en de opgedane lessen goed te borgen. Daarnaast is de politie ook vaak niet open om data beschikbaar te stellen voor externe onderzoeksdoeleinden. Dat heeft enerzijds te maken met het vertrouwelijke karakter van politiewerk, maar ook met het feit dat transparante politiepraktijken criminelen in de kaart kunnen spelen.

6.7 Conclusies en reflecties

Het aantal geïnventariseerde artikelen die de empirische ervaringen van de politie in het buitenland met overige toepassingen in kaart brengen, is beperkt. Het betreft hier wederom veel beschouwende bijdragen, met inzichten die grotendeels in lijn zijn met de observaties in de internationale literatuur over de drie clusters die in de vorige drie hoofdstukken werden belicht.

Verschillende (buitenlandse) politieonderzoekers en -experts hebben hun reflecties gedeeld tijdens digitale consultaties. Ze onderschreven het belang van het academische (en maatschappelijke) debat over de ethische kant van AI, mede omdat de politie in het buitenland ook AI-toepassingen inzet, waarover (nog) niet is gepubliceerd. Verder hebben de gesprekspartners in dat kader gewezen op de behoefte van de politie aan kaders. Mogelijke risico's op het gebied van AI zijn de dominantie van bedrijven die AI-toepassingen ontwikkelen en leveren en dat kan resulteren in ongewenste publiek-private afhankelijkheidsrelaties. Verder is naar voren gebracht dat de benaderbaarheid van de politie en het vertrouwen van burgers in de politie per land kan variëren. In landen waar de politie gewantrouwd wordt, zal er met argusogen gekeken worden naar de technologie die de politie inzet en de intenties die daaraan ten grondslag liggen. Tot slot hebben de politieprofessionals gepleit voor (meer) evaluaties en impactmetingen van AI-toepassingen door de politie, zodat de behaalde resultaten inzichtelijk(er) en transparanter worden.

In het volgende hoofdstuk wordt AI in de context van de Nederlandse politie geplaatst. Die context is van belang om internationale ervaringen met AI te kunnen vertalen in beredeneerde aandachtspunten voor de (Nederlandse) politiepraktijk.

7 AI en de Nederlandse politiecontext

7.1 Inleiding

In de voorgaande vier hoofdstukken zijn op basis van bestaande literatuur beschouwende observaties en empirische ervaringen van de politie in het buitenland met kunstmatige intelligentie voor het voetlicht gebracht. De buitenlandse bespiegelingen en ervaringen die in het buitenland zijn opgedaan, zijn niet allemaal relevant of bruikbaar voor de Nederlandse politie, omdat rekening moet worden gehouden met contextuele factoren. Belangrijke juridische kaders in de Europese Unie zijn het EVRM die de mensenrechten van burgers beschermt en de AVG die de privacy van burgers beschermt. De Nederlandse politie moet daar, net als andere politieorganisaties in de Europese Unie, rekening mee houden. Een andere relevante contextuele factor is de politiek-maatschappelijke context waarbinnen de politie opereert. In Nederland is bijvoorbeeld het vertrouwen van burgers in de politie relatief hoog. Het is in dat kader van groot belang dat AI-toepassingen binnen de politie dit vertrouwen niet aantasten. Een derde relevante factor is institutioneel van aard. In Nederland is bij de vorming van de nationale politie sprake geweest van centralisatie. In de Verenigde Staten is de politie decentraal georganiseerd. Deze context is van invloed op de wijze waarop innovaties tot stand komen.

Om de opgedane inzichten uit de internationale literatuur te kunnen vertalen naar beredeneerde aandachtspunten voor de (Nederlandse) politie zal eerst globaal aandacht moeten worden besteed aan de wijze waarop AI momenteel binnen de Nederlandse politie wordt ingezet. Deze inzichten zijn verzameld aan de hand van een beknopte literatuurstudie (paragraaf 7.2). Na de uitvoering van de internationale literatuurstudie werd een digitale focusgroep georganiseerd waarin Nederlandse politieprofessionals hebben gereflecteerd op de belangrijkste resultaten van de internationale literatuurstudie. De belangrijkste resultaten van deze focusgroep zijn vermeld in paragraaf 7.3. In paragraaf 7.4 staan de conclusies.

7.2 AI toepassingen bij de Nederlandse politie

Criminaliteits Anticipatie Systeem (CAS)

Willems & Doeleman (2014) hebben in een artikel aandacht besteed aan predictive policing in Nederland. Ze omschrijven predictive policing als het gebruik van statistische voorspellingen om te kunnen anticiperen op criminele incidenten. Deze informatie kan, afhankelijk van de acties die erop worden gebaseerd, worden gebruikt ter preventie van misdaad of het vergroten van de heterdaadkracht. Een voorwaarde voor het succesvol kunnen inzetten van predictive policing is dat gegevens over criminele activiteiten ontsloten zijn in een datawarehuis, en dat andere data hieraan gekoppeld kunnen worden (Willems & Doeleman, 2014). In het artikel wordt ook het Criminaliteits Anticipatie Systeem (CAS) behandeld. Dit systeem is ontwikkeld door de politie in Amsterdam met als doel om misdaad te voorspellen. Willems & Doeleman geven aan dat ongeveer 40 procent van de woninginbraken en 60 procent van de straatroven in Amsterdam kunnen worden voorspeld met behulp van CAS. Er werd in Amsterdam een duidelijke daling van het aantal woninginbraken geconstateerd, maar dit succes kan niet alleen aan CAS worden toegeschreven. De politie in Amsterdam heeft namelijk veel meer inspanningen geleverd om het aantal woninginbraken terug te dringen en dus naast CAS ook andere activiteiten ontplooid. Verder wijzen de auteurs op het feit dat het interpreteren van de informatie in CAS en het formuleren van geschikte acties en interventies noodzakelijkerwijs mensenwerk is en dat hiervoor capaciteit moet worden vrijgemaakt.

Van der Eijk (2021) heeft in een masterscriptie onderzoek gedaan naar het CAS. Het doel van haar onderzoek was om factoren in kaart te brengen die van invloed zijn op een succesvolle implementatie van predictive policing. Een relevante interne factor is draagvlak. Politiemensen moeten namelijk het concept omarmen en integreren in hun werkproces. Datzelfde geldt voor instituties rondom de politie (ministerie van Veiligheid en Justitie, politiek en maatschappij). Andere factoren zijn IT governance en transparantie. Transparantie is noodzakelijk om de uitkomsten te begrijpen en om fouten te signaleren en te herstellen. Het CAS is niet de enige bron van informatie die de politie gebruikt en dat is een belangrijke relativerende noot. Andere relevante factoren zijn timing (de implementatie van CAS viel samen met een reorganisatie en dus in een periode waarin er ruimte was voor verandering), de mogelijkheid om CAS in te zetten voor verschillende typen criminaliteit en dus toe te spitsen op specifieke lokale behoeften ('customatization') en het feit dat het gebruik van CAS niet werd 'opgelegd'. CAS is, in tegenstelling tot veel internationale predictive policing toepassingen, niet ontwikkeld door private partijen, maar door de politie zelf en dat geeft de politie meer zeggenschap. Van der Eijk concludeert dat de Nederlandse politiecontext, -cultuur en omgeving anders is dan elders en dat slechts één casus is onderzocht. De bevindingen kunnen daarom niet gegeneraliseerd worden. Dit vereist grondig comparatief onderzoek.

Mali e.a. (2017) hebben de landelijke pilot Predictive Policing geëvalueerd. Bij predictive policing kunnen verschillende systemen worden gebruikt. Bij de pilot werd op voorhand gekozen voor het zogenaamde CAS. Het CAS maakt gebruik van een veelheid aan gegevens om prognoses te maken. Zo gebruikt het CAS criminaliteitsgegevens en koppelt die aan andere gegevens die potentieel relevant zijn voor criminaliteit, zoals gegevens over de bevolkingssamenstelling. Een kracht van het CAS is dat veel variabelen meegenomen kunnen worden. Een kwetsbaarheid is het technisch niet beschikbaar zijn van tactisch relevante variabelen voor het CAS en het niet duidelijk hebben welke variabelen (sterk) bepalend zijn voor de voorspelling. Uit de evaluatie bleek dat het interne draagvlak voor predictive policing hoog is. Bijna 80 procent van de respondenten ervaarde predictive policing als legitiem in de zin dat het relevant is voor het politiewerk. Een knelpunt was de gebrekkige sturing in de pilotteams waardoor het potentieel van predictive policing niet optimaal werd benut. Prognoses hebben bijvoorbeeld implicaties voor de personeelsplanning. Bij de pilotteams lukte het niet om de planning structureel aan te passen aan de prognoses als gevolg van bureaucratie. De onderzoekers hebben geen aanwijzingen gevonden dat predictive policing uiteindelijk leidt tot minder (stijgende) criminaliteit (Mali e.a., 2017, p. 41). De afstand tussen wat predictive policing kan zijn en wat het in de praktijk is, is dus groot.

'Big Data' datamining

Brinkhoff (2017) heeft onderzoek gedaan naar 'Big Data' data mining door de Nederlandse politie. Daarbij werd een specifieke toepassing bestudeerd, namelijk iColumbo. Dit is een geautomatiseerd systeem waarbij op basis van specifieke zoekwoorden, profielen en analyses van Big Data op internet, gepersonaliseerde resultaten over (mogelijke) strafbare feiten inzichtelijk gemaakt kunnen worden. Deze vorm van data mining is nog geen onderwerp van een fundamenteel debat. Brinkhoff bepleit een dergelijk debat, waarbij de volgende criteria kunnen worden gehanteerd, namelijk dat deze vorm van data mining alleen wordt gebruikt bij een redelijke verdenking van strafbare feiten, dat strafzaken niet uitsluitend zijn gebaseerd op geautomatiseerde analyses van (big) data en dat officieren van justitie en rechters ook oog hebben voor de privacy van onschuldige burgers die bij geautomatiseerde analyses van (big) data ernstig in het geding kunnen zijn.

Politierobot in Amsterdam

Op dinsdag 22 februari 2022 vond in de Applestore op het Leidseplein in Amsterdam een gijzeling plaats. De gijzelnemer eiste 200 miljoen euro aan cryptovaluta. Hij schoot met een automatisch vuurwapen op toegesnelde agenten en vertelde de politie dat hij een bomvest droeg. Tijdens de gijzeling werd een speciale politierobot ingezet. De gijzelnemer had namelijk om een flesje water gevraagd en dat werd afgeleverd door een robot. Toen de gijzelaar het water moest pakken wist de gegijzelde te vluchten. Tijdens de achtervolging wist de gijzelaar te ontkomen en werd de gijzelnemer aangereden door een gepantserde auto van de Dienst Speciale Interventies (DSI). De gijzelnemer raakte daarbij zwaargewond en overleed daarna in het ziekenhuis. Alle overige betrokkenen bleven ongedeerd.[20]

Videovoertuig in Dordrecht

In Dordrecht is een proef gestart met een zogeheten videovoertuig. Dit voertuig kan worden ingezet bij incidenten in de gemeente Dordrecht. Het busje heeft onder meer een draaibare camera op de mast en een warmtebeeldsensor. De camera kan bediend worden in het voertuig zelf. Als de situatie daarom vraagt kan de camera ook bediend worden door een medewerker in de meldkamer. Daar kan op afstand worden meegekeken en ingeschat welke politie-inzet in een bepaalde situatie nodig is. Er zijn ook vier camera's op het dak van het busje geplaatst. Die een beeld van 360 graden kunnen geven. Medewerkers zijn getraind om met het voertuig te werken. Zij weten hoe ze de beelden kunnen en mogen gebruiken. De gemaakte beelden worden 28 dagen opgeslagen en daarna automatisch verwijderd. De bewaartermijn kan worden verlengd als de beelden nodig zijn voor een onderzoek.[21]

7.3 Resultaten digitale focusgroep

Op maandag 27 juni 2022 werd een online focusgroep georganiseerd met als doel om professionals binnen de Nederlandse politie te laten reflecteren op de resultaten van de internationale literatuurstudie. De deelnemers van de online focusgroep zijn vermeld in bijlage 2.

Definitie en categorisering van AI

Kunstmatige intelligentie is in de beleving van de deelnemers een 'hype' en dit betekent dat ook in de literatuur veel toepassingen AI worden genoemd, terwijl dat niet altijd het geval is of lijkt te zijn. Een belangrijk discussiepunt betrof de vraag wat nu precies onder kunstmatige intelligentie moet worden verstaan en welke concrete toepassingen daar al dan niet onder moeten worden geschaard. In de politiepraktijk en in de literatuur bestaan er verschillende opvattingen over wat AI nu precies is. De gehanteerde werkdefinitie van de High-Level Expert Group on Artificial Intelligence wordt ervaren als een tekstboekdefinitie. De definitie die de OECD hanteert, is iets breder. De deelnemers hebben aangegeven dat het belangrijk is om in het onderzoeksrapport te benoemen dat er (nog) geen consensus is over het begrip AI.

Het ontbreken van een gedeelde en eenduidige definitie had ook zijn weerslag op de discussie in de focusgroep. Een deelnemer was van mening dat predictive policing op zich niets met AI te maken heeft, terwijl deze opvatting door andere deelnemers werd betwist. Tevens werd de vraag gesteld of facial

[20] https://www.nrc.nl/nieuws/2022/02/23/zon-gijzelneming-als-deze-is-zeldzaam-in-nederland-a4093156

[21] https://www.nu.nl/tech/6216547/politie-start-proef-met-voertuig-met-draaibare-camera-en-warmtebeeldsensor.html

recognition technology wel AI is. Is de huidige toepassing van FRT niet meer dan het uitvoeren van een aangeleerd algoritme? In Nederland wordt FTR gericht gebruikt voor specifieke doeleinden en niet zoals in China om alle mensen in de gaten te houden.

Bij een smalle definitie van AI zullen er naar verwachting een beperkt aantal toepassingen bij de politie boven tafel komen. Bij een bredere definitie zullen er meer toepassingen belicht worden met de kanttekening dat er dan toepassingen belicht worden die mogelijk onterecht onder AI worden geschaard. In dit onderzoek wordt overigens een brede definitie gehanteerd en dus een breed palet aan toepassingen in het buitenland gepresenteerd.

Beladen terminologie

De thema's predictive policing, smart policing en automated policing liggen gevoelig bij de politie, vanwege (eenzijdige) associaties met (vermeende) discriminatie en robocop. Bij de gehanteerde werkdefinitie van predictive policing wordt opgemerkt dat de politie in Nederland bij predictive policing niet personen, maar gebieden in kaart brengt en daarbij de kans berekent dat in een bepaald gebied op een bepaald tijdstip iets gebeurt dat niet in de haak is. Predictive policing in Nederland moet daarom niet worden geframed als 'personal profiling'. Eigenlijk omvat predicitve policing in Nederland niet meer dan het inzetten van risicotaxatiemodellen. In het verleden werd bij preventief fouilleren gebruik gemaakt van data op persoonsniveau, maar bij deze activiteit werd de politie teruggefloten door de rechter. Voor wat betreft smart policing zou het begrip supportive policing de lading beter dekken. Robotic policing is een beladen begrip en roept vooral de associatie op van robocop. Automated policing is neutraler en minder beladen. Taal is niet neutraal. Veel artikelen beogen mee te liften op de emotie. Het vinden van een neutrale basis is lastig.

Verschillende componenten van AI

Kunstmatige intelligentie heeft volgens de deelnemers verschillende componenten. Een belangrijke component is dat AI data- en kennisgedreven is. Verder kan AI proactief en reactief worden ingezet en al dan niet ondersteunend zijn. Voor wat betreft de bestaande toepassingen binnen de Nederlandse politie werd naar voren gebracht dat AI veelal nog niet meer omvat dan taakautomatisering. Dit betreft de inzet van AI bij specifieke taken. De trend van het automatiseren van deeltaken is overigens al heel lang aan de gang. De meest geavanceerde variant van AI, namelijk superintelligentie, bestaat nog helemaal niet. Datzelfde geldt voor geheel autonome systemen. Er worden bij de politie (in Nederland) geen systemen ingezet die volledig autonoom zijn. Er zijn dus altijd mensen bij betrokken.

Technologie op zich versus het gebruik van technologie

Het is een wezenlijke vraag waar specifieke technologie concreet voor wordt gebruikt. Het is belangrijk om een onderscheid te maken tussen AI op zich (technologie) en het gebruik van AI. Bij iedere specifieke politietoepassing kan de politie overwegen om AI in te zetten, maar ook andere instrumenten. Het toepassen van AI is in dat opzicht geen wetmatige noodzakelijkheid. Bepalend is ook de intelligentie van de interventiestrategie van de politie. De politie kan slimme technologie inzetten, maar is niet slim wanneer daar dan geen slimme interventiestrategie uit voortvloeit. Het handmatig bekijken van camerabeelden is bijvoorbeeld tijdrovend en niet efficiënt.

AI in het opsporingsproces

Over AI die wordt ingezet ten behoeve van het opsporingsproces wordt nauwelijks iets gepubliceerd, omdat transparantie daarover de effectiviteit van het opsporingsproces kan belemmeren. De politie kan niet alle activiteiten publiceren, omdat criminelen ook mee kunnen lezen en "hen wil je niet wijzer maken".

Breder (keten)perspectief op AI

Veel factoren die bij smart policing zijn vermeld verwijzen niet naar de politie, maar naar steden, namelijk het concept smart city. Bij veel activiteiten die daar uit voortvloeien, bijvoorbeeld crowd management, ligt de regie niet bij de politie, maar bij andere organisaties. Daarom is het belangrijk om vanuit een breder (keten)perspectief naar AI te kijken.

Framing

In de focusgroep is gewezen op het gevaar van 'framing' in publicaties, waarbij de gevaren van AI breed worden uitgemeten, bijvoorbeeld het gevaar van de surveillance society. Het doel van de politie is niet om alle burgers in de gaten te houden, maar om criminelen op te sporen. Een andere kritische noot is dat veel mensen iets roepen over AI, terwijl ze op dat vlak geen expert zijn en dus niet goed begrijpen waar ze het over hebben.

Aandacht voor de context

Tijdens de focusgroep werd naar voren gebracht dat het belangrijk is om niet alleen onderzoek te doen naar AI, maar ook de zaken en randvoorwaarden daaromheen, bijvoorbeeld het vraagstuk van governance en de juridische randvoorwaarden waarbinnen de Nederlandse politie moet opereren. In landen als de Verenigde Staten en China zijn er minder beperkingen ten aanzien van de privacy van burgers. De politie aldaar kan daarom grotere stappen zetten op het gebied van bijvoorbeeld gezichtsherkenningstechnologie. In Europa beschermt het EVRM de mensenrechten van burgers en beschermt de AVG de privacy van burgers. Deze juridische kaders zijn van invloed op de toepassingsmogelijkheden van nieuwe technologie.

Internationale focus van literatuurstudie benadrukken

De deelnemers vinden het belangrijk dat in het onderzoeksrapport wordt benadrukt dat de inzichten en observaties louter zijn gebaseerd op internationale artikelen. Wanneer louter Nederlandstalige literatuur zou zijn bestudeerd over de ervaringen van de Nederlandse politie, dan zou er een ander beeld naar voren komen.

Risico's

Bij de genoemde risico's van predictive policing wordt naar voren gebracht dat de risico's herkenbaar zijn, maar dat dit algemene risico's betreft van het werken met algoritmen en modellen in het algemeen en dat de genoemde risico's dus een generiek karakter hebben.

Een risico dat nog niet is belicht is het ontbreken van een kosten-batenanalyse. Het is voor de politie van groot belang dat een beredeneerde afweging wordt gemaakt tussen de (verwachte) baten en de (verwachte) kosten. Concrete baten kunnen onder meer betrekking hebben op het verwerven van nieuwe inzichten of een efficiëntere inzet van de politie. Het valt op dat de (vermeende) risico's van AI in de literatuur heel veel aandacht krijgen, terwijl de kansen en de baten voor de politie doorgaans minder worden belicht. Dat is overigens wel te begrijpen. De toegevoegde waarde van AI is voor bedrijven eenvoudiger vast te stellen, dan bij de politie vanwege de mogelijke indirecte effecten van andere factoren.

Kritische succesfactoren

Een belangrijke kritische succesfactor is de aanwezigheid van een duidelijke corporate strategy op AI bij de politie. Daarnaast is een ethische verantwoorde implementatie van groot belang. Daarbij kan het raadzaam zijn om twee dimensies te onderscheiden (intern versus extern en individueel versus

collectief), zodat vier kwadranten kunnen worden ingevuld: individuele politieprofessionals, individuele burgers, de politieorganisatie en de samenleving.

7.4 Conclusies

Een belangrijke conclusie in de focusgroep is dat AI niet alleen een actueel, maar ook een beladen thema is. Verder is er (nog) geen consensus over wat precies onder AI-toepassingen bij de politie moet worden verstaan. Daarnaast werd in de focusgroep naar voren gebracht dat een onderscheid moet worden gemaakt tussen AI als technologie en het gebruik van AI door de politie. Het gebruik van AI door de politie wordt mede bepaald door contextuele factoren die per land kunnen verschillen, bijvoorbeeld juridische kaders en de wijze waarop de politie wordt aangestuurd. Wat verder opviel tijdens de focusgroep waren dat de gesprekspartners kritischer waren over de (vermeende) resultaten van predictive policing dan de literatuur. Dit is in lijn met het pleidooi om meer evaluaties en impactmetingen uit te voeren, bij voorkeur door onafhankelijke onderzoekers, zodat er onderbouwde uitspraken kunnen worden gedaan over de resultaten die met AI bij de politie worden behaald, evenals de onbedoelde neveneffecten en risico's van AI in de praktijk. Bij het meten van de impact van AI kan een onderscheid worden gemaakt tussen impact op individuele politieprofessionals, individuele burgers, politieorganisatie en samenleving. Vertrouwen en legitimiteit zijn daarbij belangrijke (ethische) ankerpunten.

8 Conclusies en aandachtspunten

8.1 Inleiding

In dit hoofdstuk worden op basis van de internationale literatuurstudie, de gesprekken die met buitenlandse politieonderzoekers zijn gevoerd en de observaties tijdens de online focusgroep algemene conclusies getrokken en de onderzoeksvragen beantwoord (paragraaf 8.2). In paragraaf 8.3 staan specifieke conclusies en daaruit afgeleide concrete aandachtspunten voor de (Nederlandse) politie.

8.2 Algemene conclusies

AI is een diffuus begrip

In de literatuur wordt AI op verschillende manieren gedefinieerd. Dat heeft ook zijn weerslag op dit onderzoek. Zowel in de begeleidingscommissie (zie bijlage 3) als tijdens de digitale focusgroep (zie bijlage 2) is er een semantische discussie gevoerd over de vraag wat AI precies is en welke toepassingen daar al dan niet onder geschaard kunnen worden. Deze literatuurstudie zal deze semantische discussie niet kunnen beslechten en dat is ook niet de insteek geweest. Een feit is dat er momenteel veel slimme innovaties worden ontwikkeld die geleidelijk hun weg vinden binnen verschillende politieorganisaties. De impact van deze innovaties is belangrijker dan de aard van de innovaties en de mate waarin AI (op welke manier dan ook gedefinieerd) is geïntegreerd in deze innovaties. AI moet daarom niet worden benaderd als een dichotomie (wel of geen AI), maar als een schaal, waarbij de mate van intelligentie kan variëren van lage tot hoge intelligentie en daarmee de mate waarin AI-systemen taken 'zelfstandig' en 'autonoom' kunnen uitvoeren.

Veel beschouwende artikelen, weinig empirisch gefundeerde artikelen

Wanneer wordt gekeken naar de verhouding tussen empirisch gefundeerde en beschouwende artikelen, dan kan worden geconcludeerd dat de meeste artikelen die zijn bestudeerd een beschouwend karakter hebben en het aantal empirisch gefundeerde artikelen relatief beperkt is. Daar liggen verschillende mogelijke verklaringen aan ten grondslag. Een eerste verklaring is dat nog volop ervaring wordt opgedaan door middel van pilots, proeftuinen en experimenten. De resultaten daarvan zijn veelal nog niet uitgekristalliseerd en belicht in wetenschappelijke literatuur. Een tweede verklaring is dat het bij de politie niet altijd gebruikelijk is om pilots en experimenten grondig te laten evalueren door externe (politie)onderzoekers. De lessen uit interne evaluaties zullen intern gedeeld worden, maar zijn niet altijd inzichtelijk voor de buitenwereld. Een derde verklaring die door politieonderzoekers naar voren werd gebracht is dat transparantie op het gebied van AI bij de politie criminelen in de kaart kan spelen. De politie heeft er geen direct belang bij om ervaringen op het gebied van AI gedetailleerd te delen met (politie)onderzoekers. De politie in verschillende landen kan dus verder zijn in haar toepassing van AI dan de bestaande (wetenschappelijke) literatuur lijkt te suggereren.

In dit onderzoek zijn verschillende onderzoeksvragen geformuleerd die hieronder beantwoord gaan worden.

Deelvraag 1: Wat zijn de (verwachte) kansen van AI voor de politie?

In de internationale literatuur wordt meer aandacht besteed aan de risico's (zie deelvraag 2) dan aan de kansen van AI. Een belangrijk en voor de hand liggen motief om AI-toepassingen in te zetten binnen

politieorganisaties in het buitenland, is het verhogen van de veiligheid van de samenleving (macroniveau) en het verhogen van de effectiviteit en efficiency van de politieorganisatie (mesoniveau). Deze (verwachte) kansen spelen een rol bij predictive policing, smart policing & automated policing. De (verwachte) voordelen van kunstmatige intelligentie voor individuele politieprofessionals en individuele burgers wordt in de literatuur niet of nauwelijks belicht (microniveau). Een uitzondering vormen specifieke toepassingen op het gebied van automated policing, namelijk gerobotiseerde apparaten die gevaarlijk werk kunnen overnemen en daarmee het politiewerk veiliger kunnen maken voor individuele agenten (microniveau). Het veiliger maken van de samenleving heeft in dat opzicht ook een individuele dimensie. Voor wat betreft het verhogen van de effectiviteit, moet worden gedacht aan het voorspellende potentieel van AI. De effectiviteit van de politie kan door middel van predictive policing worden vergroot door locatiegerichte criminaliteit te voorspellen en daar gerichte interventies op te plegen, en door verdachte personen of situaties gericht in de gaten te houden. Smart surveillance kan gericht zijn op het monitoren van individuele personen. De inzet van AI ter verhoging van de efficiency omvat onder meer het inzetten van technologie, zodat de politie meer kan bereiken met minder menskracht. Bij automated policing wordt daarbij in de literatuur soms ook een individuele dimensie belicht: AI kan saaie en routinematige taken van politiemedewerkers overnemen, zodat zij hun tijd efficiënter kunnen benutten. In de literatuur wordt deze kans soms ook opgevat als een bedreiging. Daarvan is sprake wanneer AI mensen vervangt en overbodig maakt. In de internationale literatuur zijn er geen concrete aanwijzingen dat dit laatste bij de politie het geval zou zijn. Kansen op microniveau worden weliswaar belicht in de internationale literatuur, maar minder frequent als de kansen op meso- en macroniveau.

Deelvraag 2: Wat zijn de (verwachte) risico's van AI voor de politie?

In het algemeen wordt in de internationale literatuur meer aandacht besteed aan de risico's dan de kansen van AI. Belangrijke (verwachte) generieke risico's die in de literatuur het vaakst zijn benoemd, hebben betrekking op discriminatie, privacy en de implicaties van fouten die AI-systemen kunnen maken.

Discriminatie kan onbedoeld optreden wanneer er sprake is van 'biases' in data of algoritmen die aan AI-systemen ten grondslag liggen. AI-systemen leren namelijk op basis van historische data en als er 'biases' in deze data zitten, dan liggen deze ook ten grondslag aan het leren van het systeem en dat is niet wenselijk. Een ander risico is dat de *privacy* van burgers wordt aangetast. Op het veiligheidsdomein is in dat kader van oudsher sprake van een dilemma tussen het verhogen van veiligheid en het inleveren van privacy. Die afweging is uiteindelijk geen wetenschappelijke, maar een politieke keuze. Uit de internationale literatuur blijkt dat de mate van aantasting van privacy per toepassing en per organisatie kan verschillen. Bij predictive policing kan bijvoorbeeld de focus liggen op risicoplekken en risicopersonen. Bij het voorspellen van criminaliteit op 'hotspots' is de aantasting van privacy niet aan de orde, maar bij het voorspellen van criminele gedragingen van personen die op een watch list staan wel. In Nederland ligt de focus op 'places', maar in de Verenigde Staten zijn ook voorbeelden van predictive policing gevonden waar de focus lag op 'persons'. Dit voorbeeld laat zien dat de inzet en focus van specifieke tools per politieorganisatie kan verschillen en daarmee ook de mate waarin specifieke risico's zich kunnen manifesteren. De privacy van burgers kan zichtbaar, maar ook heimelijk worden aangetast. Bij slimme camera's die zichtbaar in de publieke ruimte zijn geplaatst, kunnen burgers weten dat er beelden worden geregistreerd, maar dit is niet het geval bij drones die op afstand beeldmateriaal verzamelen. Bij het gericht volgen van verdachte personen is dat onvermijdelijk en minder bezwaarlijk (omdat hier een motivering en zorgvuldige afweging aan ten grondslag ligt) dan bij het ongericht volgen van onschuldige burgers. Een ander risico is de *kans op fouten*. Hoewel mensen ook fouten kunnen maken, zijn er sterke aanwijzingen dat fouten in systemen

minder worden geaccepteerd in de samenleving dan menselijke fouten. Een aannemelijke verklaring is dat bij menselijke fouten ook mensen aansprakelijk kunnen worden gesteld, terwijl dat bij AI-systemen veel lastiger is. Fouten in AI-systemen kunnen bijvoorbeeld worden toegeschreven aan de bouwers van deze systemen, maar ook aan de gebruikers en dat kunnen mensen zijn die de data onjuist interpreteren en op basis daarvan foute of onjuiste interventies plegen. Fouten in AI-systemen kunnen ingrijpende gevolgen hebben voor burgers. Ze kunnen bijvoorbeeld onterecht in risicoprofielen belanden of ten onrechte als verdachte personen worden aangemerkt.

Risico's die in iets mindere mate zijn vermeld in de literatuur hebben betrekking op doelverschuiving, aantasting van discretionaire ruimte, aantasting van de kwaliteit van interacties, dominantie van private bedrijven en militarisering van de politie. *Doelverschuiving* treedt op wanneer data voor andere doeleinden worden gebruikt dan waarvoor ze verzameld zijn. Een voorbeeld is kentekenregistratie door slimme camera's. Het doel daarvan kan zijn om voertuigen te detecteren, maar dit doel kan ook verschuiven naar het detecteren van verdachte personen in deze voertuigen. In dat laatste geval kan de privacy van burgers in het geding zijn. Doorgaans is er een wettelijke basis die de doelbinding bepaalt en dit verkleint de kans op onrechtmatige dataverzameling. Verder kan AI resulteren in een *aantasting van discretionaire ruimte* van professionals binnen de politie. De mate waarin de handelingsruimte van politieprofessionals wordt ingeperkt kan per toepassing verschillen. In sommige gevallen wordt er veel gewicht toegekend aan het gezonde verstand van professionals bij de politie, terwijl er in andere gevallen (blind) wordt vertrouwd op AI-systemen. Dat verschil werd bijvoorbeeld zichtbaar bij predictive policing, waarbij uit de literatuur bleek dat de ruimte voor het professionele menselijke oordeel per politieorganisatie kan variëren. Het is belangrijk dat er voldoende ruimte is voor het gezond verstand van professionals, om eventuele systeemfouten tijdig te signaleren en te voorkomen. AI kan een negatieve impact hebben op de *kwaliteit van de interacties* tussen de politie en de samenleving. Digitaal contact kan als afstandelijk en minder prettig worden ervaren dan persoonlijk contact, maar dat is mede afhankelijk van de specifieke context. Voor standaardaangiften kan digitaal contact een prima alternatief zijn, terwijl er bij ingrijpende gebeurtenissen juist behoefte kan zijn aan persoonlijke contacten met de politie. Het is daarom belangrijk dat de burgers via verschillende communicatiekanalen de politie kunnen benaderen. In de literatuur over (digitale) dienstverlening wordt in dat kader gewezen op het belang van multi channeling. Burgers zijn immers een belangrijke informatiebron voor de politie. Een ander risico is de *dominantie van private bedrijven.* In de Verenigde Staten wordt bijvoorbeeld veel AI-technologie geleverd door private partijen en dit kan resulteren in een eenzijdige afhankelijkheidsrelatie tussen politieorganisaties en de leveranciers van AI-technologie. Een risico dat specifiek is genoemd bij automated policing in de Verenigde Staten is *militarisering van de politie*. Dit risico werd bijvoorbeeld expliciet in de Amerikaanse literatuur benoemd bij de inzet van een bomrobot door de politie in Dallas. Militarisering kan de afstand tussen burgers en de politie vergroten en in het uiterste geval, ervoor zorgen dat burgers en de politie letterlijk lijnrecht tegenover elkaar komen te staan. In andere landen zijn nog geen bomrobots ingezet, maar niemand kan uitsluiten dat dit in de toekomst gebeurt.

Deelvraag 3: Wat zijn de kritische succesfactoren bij de toepassing van AI door de politie?

Uit de internationale literatuur zijn tien kritische succesfactoren afgeleid. Deze factoren zijn bepalend bij het effectief inzetten van AI door de politie (en in de keten betrokken organisaties). De **eerste** kritische succesfactor is *de acceptatie van AI* en andere nieuwe technologieën binnen de politie en de samenleving. De **tweede** kritische succesfactor betreft *de kwaliteit en de kwantiteit van data*. Hoe meer (hoogwaardige) data de politie bezit, hoe optimaler het leerproces van AI-systemen, omdat de kwaliteit en effectiviteit van dit leerproces immers in belangrijke mate wordt bepaald door de hoeveelheid en de kwaliteit van de data waarover de politie beschikt. Tegelijkertijd kan de politie,

afhankelijk van de context, niet ongelimiteerd data verzamelen. In Europa, dus ook in Nederland, zijn de EVRM en de AVG bijvoorbeeld van invloed op de hoeveelheid en aard van de gegevens die de politie mag verzamelen. Een **derde** kritische succesfactor is de *IT-infrastructuur*. De inzet van AI door de politie vereist een interne IT-infrastructuur die daarvoor is toegerust en dus toereikend is om grote hoeveelheid data te verwerken en te analyseren. Een **vierde** kritische succesfactor betreft de *verdere professionalisering* binnen de politie. Het gebruik van AI binnen politieorganisaties vereist ook nieuwe kennis, vaardigheden en competenties van politieprofessionals. Dit betreft onder meer het correct invoeren van data in AI-systemen, het juist interpreteren van data in AI-systemen en het op basis daarvan effectieve interventies te plegen. De vereiste kennis, vaardigheden en competenties moeten tijdens de opleiding of via (bij)scholingstrajecten overgedragen worden aan politieprofessionals. De **vijfde** kritische succesfactor betreft *menselijke oordeelsvorming*. Het is belangrijk dat er binnen politieorganisaties voldoende ruimte is voor het menselijke oordeel als dubbelcheck om fouten en biases te signaleren. Uit de bestudeerde literatuur blijkt dat de ruimte voor het professionele oordeel bij politieorganisaties kan variëren. In sommige gevallen wordt er in belangrijke mate (blind) vertrouwd op de uitkomsten van AI-systemen, terwijl er bij andere cases meer gewicht wordt toegekend aan het 'gezond verstand' van politieprofessionals. De **zesde** kritische succesfactor is *transparantie*. Veel AI-systemen fungeren in zekere mate als 'black box' waardoor uitkomsten voor experts vaak wel, maar voor leken vaak niet (goed) te doorgronden zijn. Dat probleem kan worden vergroot wanneer politieorganisaties bij AI-toepassingen afhankelijk zijn van externe leveranciers. Als de politie op basis van AI specifieke interventies pleegt, dan is het belangrijk dat dit goed kan worden uitgelegd aan de samenleving en de burgers. De **zevende** kritische succesfactor is *wettelijke inkadering*. Discriminatie en de aantasting van de privacy van burgers zijn in de internationale literatuur in dat kader benoemd als de belangrijkste risico's. Daarom is het belangrijk dat er voldoende juridische waarborgen zijn om discriminatie en de onnodige aantasting van privacy van burgers te voorkomen. Vanwege opsporingsbelangen kan de privacy van (verdachte) burgers in het geding zijn. In dat geval is een belangrijke rol als 'waakhond' weggelegd voor toezichthouders. De **achtste** kritische succesfactor is het *periodiek evalueren* van de ervaringen die met AI worden opgedaan. In de literatuur zijn weinig tot geen artikelen gevonden die inzicht bieden in evaluaties die binnen de politie zijn uitgevoerd. Hiermee is niet gezegd dat er niet wordt geëvalueerd, maar in dat geval worden de lessen in beperkte kring (intern) gedeeld, terwijl bij meer transparantie het leerpotentieel zou kunnen worden verhoogd. Hiermee is niet gezegd dat er tot in detail gerapporteerd moet worden over de bevindingen, omdat een dergelijke transparantie criminelen in de kaart kan spelen. Op basis van de uitgevoerde evaluaties kunnen ook beredeneerde kosten-batenanalyses worden uitgevoerd waarbij de verwachte opbrengsten en vereiste investeringen (hardware en software) tegen elkaar worden afgewogen. De **negende** kritische succesfactor heeft betrekking op *ethische richtlijnen*. In de internationale literatuur is in dat kader gewezen op drie principes, namelijk suitability, necessity & proportionality. Bij iedere AI-toepassing moet dus de vraag worden gesteld of de tool passend, noodzakelijk en proportioneel is. In de Europese Unie zijn de ethische richtlijnen voor betrouwbare kunstmatige intelligentie een belangrijke ethische basis (Europese Commissie, 2019). De EC onderscheidt vier ethische beginselen, namelijk respect voor menselijke autonomie, preventie van schade, rechtvaardigheid en verantwoording. De **tiende** kritische succesfactor is *(digitale) dataveiligheid*. Naarmate de hoeveelheid digitale data die de politie verzamelt en bewerkt toeneemt, neemt ook het belang van dataveiligheid toe. Het is van groot belang dat (privacygevoelige) data binnen politieorganisaties op een veilige manier worden gedeeld en opgeslagen, en dat derden (bijvoorbeeld hackers of infiltranten) zich niet ongezien toegang weten te verschaffen tot deze data.

Deelvraag 5: Welke rol spelen contextuele factoren bij de mogelijke inzet van AI?

In de internationale literatuur wordt er, veelal indirect, aandacht besteed aan contextuele factoren. Een organisatorische factor is de mate van centralisatie van de politie. Bij een gecentraliseerd politieapparaat is er meer regie bij de ontwikkeling en toepassing van AI, terwijl bij een gedecentraliseerd politieapparaat organisatieonderdelen meer autonomie hebben. Een culturele factor betreft de politiecultuur. In het ene land is de afstand tussen de politie en burgers groter dan in het andere land. In de Verenigde Staten is die afstand bijvoorbeeld groot. Deze afstand wordt in de Verenigde Staten verder vergroot door de 'militarisering' van de politie waarbij de politie en burgers vaak lijnrecht tegenover elkaar staan. Een maatschappelijke factor dat hiermee samenhangt is de mate van vertrouwen van burgers in de politie. Er zijn landen waar burgers een groot wantrouwen hebben richting de politie en er zijn landen waar sprake is van (meer) wederzijds vertrouwen tussen politie en burgers. Een juridische factor betreft de wettelijke kaders waarbinnen de politie moet opereren. Deze kaders kunnen per land verschillen. In de Europese Unie zijn het Europees Verdrag voor de Rechten van de Mens (EVRM) en de Algemene verordening gegevensbescherming (AVG) belangrijke kaders om de mensenrechten en privacy van burgers te beschermen. Deze kaders hebben invloed op de toepassingsmogelijkheden van AI door de politie binnen deze landen. In landen als de Verenigde Staten zijn er minder privacywaarborgen, om nog maar te zwijgen over landen als China, waar grote stappen lijken te worden gezet met AI, omdat de privacy van burgers voor de overheid geen belemmering vormt.

De Nederlandse politiecontext

In hoofdstuk 7 is er (globaal) aandacht besteed aan contextuele factoren die van toepassing zijn op de Nederlandse politie. Met deze factoren moet namelijk rekening worden gehouden om de internationale inzichten te vertalen naar beredeneerde lessen voor de (Nederlandse) politie. Er is in de contextuele factoren een onderscheid te maken in juridische, organisatorische, maatschappelijke en institutionele factoren.

Een relevante contextuele juridische factor voor de Nederlandse politie (en andere politieorganisaties in de Europese Unie) zijn de zojuist genoemde EVRM en AVG. De politie in de Europese Unie, inclusief Nederland, kan dus AI niet onbeperkt inzetten en moet de mensenrechten en privacy van burgers in de Europese Unie respecteren. Een relevant juridisch kader voor de Nederlandse politie is ook de Wet politiegegevens (Wpg). De Wpg regelt de verwerking van persoonsgegevens voor de uitoefening van de politietaak door onder meer de Nationale Politie, de bijzondere opsporingsdiensten, de Koninklijke marechaussee en de Rijksrecherche.

Een relevante contextuele organisatorische factor voor de Nederlandse politie is de mate van centralisatie. In Nederland is er als gevolg van de reorganisatie tot de Nationale Politie sprake van een hoge mate van centralisatie. Dit betekent in principe dat in Nederland de toepassingen op het AI centraal worden ontwikkeld. Tegelijkertijd is er ook ruimte voor decentrale innovaties bij de politie-eenheden. In de landen als de Verenigde Staten ontbreekt centrale regie en hebben politieorganisaties een hoge mate van decentrale autonomie en kunnen er dus grote verschillen bestaan in de mate waarin en de wijze waarop AI-toepassingen worden geïmplementeerd.

Een relevante contextuele maatschappelijke factor voor de Nederlandse politie is de mate van vertrouwen. In Nederland hebben burgers relatief veel vertrouwen in de politie. In landen als de Verenigde Staten is het vertrouwen van burgers in de politie aanzienlijk lager. De mate van vertrouwen is van invloed op de ruimte die de politie heeft om AI-toepassingen te implementeren. Het is namelijk cruciaal dat nieuwe toepassingen het vertrouwen van burgers in de politie niet aantasten, omdat dit ten koste gaat van de slagkracht en effectiviteit van de politie. Wanneer burgers minder vertrouwen

hebben in de politie, dan zal de bereidheid om aangifte te doen bij de politie of om informeel gegevens te delen met de politie dalen.

Een relevante institutionele factor voor de Nederlandse politie is de inbedding in de veiligheidsketen. In de bestudeerde artikelen is de politie vaak als geïsoleerde casus benaderd, terwijl politieorganisaties wereldwijd een onderdeel zijn van de veiligheidsketen. Het toepassen van AI door een specifieke ketenpartner kan doorwerken in de hele veiligheidsketen. Een concreet voorbeeld is de bewijslast die de politie met AI kan vergaren. De vraag is in hoeverre dit bewijsmateriaal wordt erkend door rechters. Daarom is het belangrijk dat ketenpartners ook anticiperen op innovaties die binnen de veiligheidsketen worden uitgerold en dat de politie de ketenpartners (pro)actief betrekt bij innovaties binnen de eigen organisatie (zie les 5).

8.3 Specifieke conclusies en aandachtspunten

Op basis van deze literatuurstudie kunnen vijf specifieke conclusies worden getrokken waar vijf concrete aandachtspunten uit zijn afgeleid.

Eerste conclusie: De impact van AI op het microniveau is onderbelicht.

Het valt op dat in de bestudeerde literatuur aanzienlijk meer aandacht wordt besteed aan de impact van AI op macro- en mesoniveau, terwijl de impact van AI op individuele politieprofessionals en individuele burgers in veel mindere mate wordt belicht, terwijl uiteindelijk individuele ervaringen bepalend zijn voor het draagvlak voor AI. Zowel politieprofessionals als burgers zullen uiteindelijk ontvankelijk moeten zijn voor specifieke toepassingen. Daarom is het belangrijk om bij de ontwikkelfase en implementatie van nieuwe technologie ook de ervaringen van individuele politieprofessionals en burgers in kaart te brengen. Een concreet aandachtspunt is dat de focus in de internationale literatuur (en dus ook van politieonderzoekers en politieorganisaties) moet worden verlegd naar individuele stakeholders op wie de technologie impact heeft, dus specifiek burgers en politiemedewerkers. Die impact is mede afhankelijk van de context en de specifieke AI-toepassing. Het is verder van groot belang dat de techniek (AI) in balans is met menselijke kennis en verwachtingen. De professionaliteit van politiemensen moet niet worden onderschat. Vanuit deze overweging vervangt AI de politieprofessionals niet, maar ondersteunt hen op basis van complementariteit.

Tweede conclusie: Veel beschouwend onderzoek, weinig empirisch onderzoek.

Op basis van de bestudeerde internationale literatuur is geconcludeerd dat het aantal empirisch gefundeerde artikelen schaars is. Datzelfde geldt voor de mate waarin onafhankelijke externe evaluaties naar concrete AI-toepassingen door de politie worden belicht in de internationale literatuur. Er wordt door politieorganisaties in binnen- en buitenland volop geëxperimenteerd met nieuwe toepassingen in de vorm van pilots, maar, afgaand op de bestudeerde literatuur, wordt er over de resultaten van de evaluaties niet of nauwelijks gepubliceerd. Voor zover het niet botst met operationele belangen, is het van groot belang dat de ervaringen worden gepubliceerd. Dit helpt politieorganisaties bij het opstellen van een beredeneerde implementatiestrategie. Empirisch onderzoek kan ook behulpzaam zijn bij het maken van zorgvuldige en evidence-based afwegingen met betrekking tot de mate waarin en de wijze waarop AI wordt ingezet. Ook empirisch gefundeerde lessen die buiten de politie met AI worden opgedaan, kunnen waardevol zijn voor politieorganisaties. Actoren moeten daarbij niet zelf het wiel uitvinden, maar ook leren van elkaars ervaringen en activiteiten op elkaar afstemmen.

Derde conclusie: Veel ethische vragen, weinig maatschappelijk debat.

Uit de internationale literatuurstudie blijkt dat AI de nodige ethische vragen oproept. Daarom is het belangrijk dat AI op een beredeneerde, transparante en verantwoorde manier wordt ingezet en dat er sprake is van toezicht en controle. Dit kan in de vorm van audits en periodieke evaluaties. In de internationale literatuur wordt systematisch gepleit voor een debat over AI en het opstellen van kaders, waarbij ethische en juridische aspecten belangrijke aandachtspunten zijn. Zowel het debat als het bepalen van de kaders moeten voortdurend worden gevoerd. Deze discussie is noodzakelijk om de ethische grenzen bij de toepassing van AI te bepalen. Dit debat is breder dan de toepassing van AI op het veiligheidsdomein, maar omvat ook de toepassing van AI op andere domeinen, bijvoorbeeld binnen het 'smart city' concept. Een debat kan ook behulpzaam zijn om het maatschappelijk draagvlak voor AI inzichtelijk te maken en bezwaren van burgers voor het voetlicht te brengen.

Vierde conclusie: Interne bedrijfsvoering onderbelicht.

Zoals eerder aangegeven, is er weinig tot geen internationaal onderzoek uitgevoerd naar de impact van AI op microniveau. Dit betreft onder andere de impact op de benodigde competenties, kennis en digitale vaardigheden van politieprofessionals, het vraagstuk van de opleiding, werving professionalisering van politiemedewerkers, de arbeidssatisfactie van medewerkers, de benodigde IT-infrastructuur en informatiemanagement. Deze les is conform een literatuurstudie die eerder werd uitgevoerd (De Kool, Vermeeren & Steijn, 2020). In het betreffende onderzoek werd gepleit om bij het meten van de impact van AI de focus te verbreden naar de interne bedrijfsvoering (PIOFACH) en AI niet louter te benaderen als technologische uitdaging, maar ook als een menselijke en organisatorische verandermanagementopgave.

Vijfde conclusie: Weinig onderzoek naar impact van AI op (bredere) veiligheidsketen.

In de bestudeerde literatuur zijn AI-toepassingen belicht die binnen de politieorganisaties zijn of worden uitgevoerd. Daarbij is er nauwelijks aandacht voor de bredere impact in de veiligheidsketen. In een eerder onderzoek hebben wij in dat kader gewezen op de impact van een slimmer en effectiever aangifteproces op het OM (De Kool, Vermeeren & Steijn, 2020). Immers, hoe beter en completer de aangiftedossiers zijn, hoe groter de kans dat het OM effectief met deze dossiers aan de slag kan. Dit betekent dat de politie en het OM ook voldoende capaciteit moeten hebben om meer dossiers af te handelen. Eenzelfde redenering kan worden opgezet voor de AI-toepassingen die in deze internationale literatuurstudie zijn belicht. AI-toepassingen die door de politie effectief worden ingezet, kunnen de werklast van ketenpartners (OM, CJIB en FIOD bijvoorbeeld) verhogen. De politie moet AI niet alleen benaderen vanuit het eigen organisatieperspectief, maar het bredere technologische ecosysteem in ogenschouw nemen. Dit impliceert dat ook verkokering binnen organisaties en tussen organisaties op het veiligheidsdomein wordt doorbroken en actoren binnen en buiten het veiligheidsdomein intensiever met elkaar samenwerken, digitale data delen (binnen de geldende juridische kaders) en gezamenlijk innoveren. Ketensamenwerking met andere actoren is noodzakelijk om criminaliteit effectief aan te pakken. Dat geldt dus ook bij het ontwikkelen en implementeren van AI-technologie in de veiligheidsketen.

Geraadpleegde literatuur

Acevedo, J. J., Arrue, B. C., Diaz-Banez, J. M., Ventura, I., Maza, I., & Ollero, A. (2014). One-to-one coordination algorithm for decentralized area partition in surveillance missions with a team of aerial robots. *Journal of Intelligent & Robotic Systems*, *74*(1), 269-285.

Afzal, M., & Panagiotopoulos, P. (2020, August). Smart policing: A critical review of the literature. In *International Conference on Electronic Government* (pp. 59-70). Springer, Cham.

Ali, W. B. (2016). Big data-driven smart policing: big data-based patrol car dispatching. *Journal of Geotechnical and Transportation Engineering*, *1*(2), 1-6.

Almeida, D., Shmarko, K., & Lomas, E. (2021). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. AI and Ethics, 1-11.

Amnesty International (2020) *We sense trouble: automated discrimination and mass surveillance in predictive policing.*

Andrejevic, M., & Gates, K. (2014). Big data surveillance: Introduction. *Surveillance & Society*, *12*(2), 185-196.

Asaro, P. (2016). " Hands up, don't shoot!" HRI and the automation of police use of force. *Journal of human-robot interaction*, *5*(3), 55-69.

Asaro, P. M. (2019). AI ethics in predictive policing: From models of threat to an ethics of care. *IEEE Technology and Society Magazine*, *38*(2), 40-53.

Babuta, A., Oswald, M., & Rinik, C. (2018). Machine Learning Algorithms and Police Decision-Making. *Legal, Ethical, and Regulatory Challenges*, 3-18.

Bakker, B. e.a. (2021) *Het technologisch ecosysteem van AI in Nederland*, WRR: Den Haag (Working Paper).

Baldwin, P., Fackrell, G., Glaude, T., Smith, S., Batson, C., Sousa, W., & Pace, S. (2014). Las Vegas smart policing initiative: Impact of police saturation. *US Department of Justice*.

Benbouzid, B. (2019). To predict and to manage. Predictive policing in the United States. *Big Data & Society*, *6*(1), 2053951719861703.

Bennett Moses, L., & Chan, J. (2018). Algorithmic prediction in policing: assumptions, evaluation, and accountability. *Policing and society*, *28*(7), 806-822.

Bethel, C. L., Carruth, D., & Garrison, T. (2012, November). Discoveries from integrating robots into SWAT team training exercises. In *2012 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR)* (pp. 1-8). IEEE.

Big Brother Watch (2018) Face off. The lawless growth of facial recognition in UK policing. https://www.bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf.

Blount, K. (2017). Body worn cameras with facial recognition technology: when it constitutes a search. *Crim. L. Prac.*, *3*, 61.

Bond, B. J., Hajjar, L., Ryan, A., & White, M. D. (2014). Lowell, Massachusetts, Smart Policing Initiative: Reducing property crime in targeted hot spots. *Alexandria, VA: CNA Corporation and Bureau of Justice Assistance, US Department of Justice*.

Bosse, T. (2019). *Sociale kunstmatige intelligentie.* Radboud Universiteit (oratie).

Bradford, B., Yesberg, J. A., Jackson, J., & Dawson, P. (2020). Live facial recognition: Trust and legitimacy as predictors of public support for police use of new technology. *The British Journal of Criminology*, *60*(6), 1502-1522.

Braga, A. A., & Schnell, C. (2013). Evaluating place-based policing strategies: Lessons learned from the Smart Policing Initiative in Boston. *Police quarterly*, *16*(3), 339-357.

Braga, A. A. (2020). Conclusion: Body-worn cameras, surveillance, and police legitimacy. In *Police on Camera*m, Routledge. pp. 237-245.

Brakel, R. van (2021). How to Watch the Watchers? Democratic Oversight of Algorithmic Police Surveillance in Belgium. *Surveillance & Society*, *19*(2), 228-240.

Brantingham, P. J. (2018). The logic of data bias and its impact on place-based predictive policing. *Ohio St. J. Crim. L.*, *15*, 473.

Brantingham, P. J., Valasik, M., & Mohler, G. O. (2018). Does predictive policing lead to biased arrests? Results from a randomized controlled trial. *Statistics and public policy*, *5*(1), 1-6.

Brayne, S. (2017). Big data surveillance: The case of policing. *American sociological review*, *82*(5), 977-1008.

Brennan-Marquez, K. (2017). Big data policing and the redistribution of anxiety. *Ohio St. J. Crim. L.*, *15*, 487.

Brinkhoff, S. (2017). Big data data mining by the Dutch police: Criteria for a future method of investigation. *European Journal for Security Research*, *2*(1), 57-69.

Bud, T. K. (2016). The rise and risks of police body-worn cameras in Canada. *Surveillance & Society*, *14*(1), 117-121.

Bui, J. (2017). Body-Worn Cameras: Reducing Citizen Complaints and Improving Relationships. *Themis: Research Journal of Justice Studies and Forensic Science*, *5*(1), 1.

Calo, M. R. (2020). 12 robots and privacy. In *Machine Ethics and Robot Ethics* (pp. 491-505). Routledge.

Cath, C. (2018). Governing artificial intelligence: ethical, legal and technical opportunities and challenges.

Catte, R. (2017). Twenty first century policing: an evaluation of the Winnipeg Police Service Smart Policing Initiative.

Chan, J., & Bennett Moses, L. (2016). Is big data challenging criminology?. *Theoretical criminology*, *20*(1), 21-39.

Chan, J., & Bennett Moses, L. (2017). Making sense of big data for security. *The British journal of criminology*, *57*(2), 299-319.

Cortes, A. L. L., & Silva, C. F. (2021). Artificial Intelligence Models for Crime Prediction in Urban Spaces. *Machine Learning and Applications: An International Journal (MLAIJ) Vol*, *8*.

Crow, M. S., Snyder, J. A., Crichlow, V. J., & Smykla, J. O. (2017). Community perceptions of police body-worn cameras: The impact of views on fairness, fear, performance, and privacy. *Criminal justice and behavior*, *44*(4), 589-610.

Currie, M., Paris, B. S., Pasquetto, I., & Pierre, J. (2016). The conundrum of police officer-involved homicides: Counter-data in Los Angeles County. *Big Data & Society*, *3*(2), 2053951716663566.

Davis, J. e.a. (forthcoming) "Five Ethical Challenges for Data-Driven Policing" (essay).

Dechesne, F., Dignum, V., Zardiashvili, L., & Bieger, L. J. (2019). *AI & Ethics at the Police,* white paper, Universiteit Leiden/ TU Delft.

Degeling, M., & Berendt, B. (2018). What is wrong about Robocops as consultants? A technology-centric critique of predictive policing. *Ai & Society*, *33*(3), 347-356.

Demir, M., Apel, R., Braga, A. A., Brunson, R. K., & Ariel, B. (2020). Body worn cameras, procedural justice, and police legitimacy: A controlled experimental evaluation of traffic stops. *Justice quarterly*, *37*(1), 53-84.

Deskundigengroep op hoog niveau inzake kunstmatige intelligentie (2018) *Ethische richtsnoeren voor betrouwbare KI*, Brussel.

Dignum, M. V., & van den Hoven, J. (2016). Reflecties op het verantwoord gebruik van kunstmatige intelligentie. *Justitiele Verkenningen*, *42*(3).

Disch, K. (2015) *Kunstmatige Intelligentie: vriend of vijand?* Bachelorscriptie, Faculteit Wijsbegeerte, Universiteit Leiden.

Dixon Jr, J. H. B. (2021). Artificial Intelligence: Benefits and Unknown Risks. *Judges' Journal*, *60*(1).

Dodd, V. (2014). Police force spends £25m on switch to technology-led crime-fighting. The Guardianhttps://www.theguardian.com/uk-news/2014/jul/21/west-midlandspolice-technology-led-crime-fighting.

Doherty, J. B. (2016). Us vs. them: The militarization of American law enforcement and the psychological effect on police officers and civilians. *S. Cal. Interdisc. LJ*, *25*, 415.

Drenth, A., & Van Steden, R. (2017). Ervaringen van straatagenten met het Criminaliteits Anticipatie Systeem. *Het Tijdschrift voor de Politie*, *79*(3), 6-10.

Egbert, S. (2019). Predictive policing and the platformization of police work. *Surveillance & Society*, *17*(1/2), 83-88.

Egbert, S., & Leese, M. (2021). *Criminal Futures: Predictive Policing and Everyday Police Work*, Taylor & Francis.

Eijk, L. van der (2021) *A successful implementation of predictive policing: An analysis of the Dutch police working with CAS*, Universiteit Leiden (masterscriptie).

Ekaabi, M. A., Khalid, K., Davidson, R., Kamarudin, A. H., & Preece, C. (2020). Smart policing service quality: conceptualisation, development and validation. *Policing: An International Journal*.

Elluri, L., Mandalapu, V., & Roy, N. (2019, June). Developing Machine Learning Based Predictive Models for Smart Policing. In *2019 IEEE International Conference on Smart Computing (SMARTCOMP)* (pp. 198-204). IEEE.

Est, R. van & L. Kool red. (2015) *Werken aan de robotsamenleving. Visies en inzichten uit de wetenschap over de relatie technologie en werkgelegenheid*, Rathenau Instituut: Den Haag.

Europese Commissie. (2018). *Artificial Intelligence for Europe*, Brussel, https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe

European Commission (2021), Proposal for a *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS,* Brussel.

Fallik, S. W., Deuchar, R., & Crichlow, V. J. (2020). Body-worn cameras in the post-Ferguson era: An exploration of law enforcement perspectives. *Journal of police and criminal Psychology*, *35*(3), 263-273.

Fan, M. D. (2018). Body cameras, big data, and police accountability. *Law & social inquiry*, *43*(4), 1236-1256.

Farrar, W. A. (2013). *Video recordings of police-citizen encounters by officers wearing body-worn video cameras: Leading a randomized control trial. Unpublished master's thesis).* Fitzwilliam College, University of Cambridge, Cambridge, England.

Feeney, M. (2016). Surveillance takes wing: Privacy in the age of police drones. *Cato Institute Policy Analysis*, (807).

Feldstein, S. (2019). The road to digital unfreedom: How artificial intelligence is reshaping repression. *Journal of Democracy*, *30*(1), 40-52.

Ferguson, A. G. (2012). Predictive policing and reasonable suspicion. *Emory LJ*, *62*, 259.

Ferguson, A. G. (2015). Big data and predictive reasonable suspicion. *U. Pa. L. Rev.*, *163*, 327.

Ferguson, A. G. (2017a). Policing predictive policing. *Wash. UL Rev.*, *94*, 1109.

Ferguson, A. G. (2017b). *The rise of big data policing*. New York University Press.

Ferguson, A. G. (2021) Facial Recognition and the Fourth Amendment. *Minn. L. Rev.*, *105*, 1105-1210.

Floridi, Luciano and Taddeo, Mariarosaria, What is Data Ethics? (November 14, 2016). Phil. Trans. R. Soc. A, Volume 374, Issue 2083, December 2016, Available at SSRN: https://ssrn.com/abstract=2907744

Fügener, A., J. Grahl, A. Gupta & W. Ketter (2021) Cognitive Challenges in Human–Artificial Intelligence Collaboration: Investigating the Path Toward Productive Delegation. *Information Systems Research* 33(2):678-696.

Fussey, P., & Murray, D. (2019). Independent report on the London Metropolitan Police Service's trial of live facial recognition technology, Human Rights Centre, University of Essex.

Fussey, P., Davies, B., & Innes, M. (2021). 'Assisted'facial recognition and the reinvention of suspicion and discretion in digital policing. *The British Journal of Criminology*, *61*(2), 325-344.

Garvie, C., Bedoya, A. M., & Frankle, J. (2019). The perpetual line-up. Unregulated police face recognition in America. Georgetown Law Center on Privacy & Technology.

Gettinger, D., & Michel, A. H. (2016). Law Enforcement Robots Datasheet. *Center for the Study of the Drone, Bard College*, 55-56.

Gkougkoudis, G., Pissanidis, D., & Demertzis, K. (2022). Intelligence-Led Policing and the New Technologies Adopted by the Hellenic Police. *Digital*, *2*(2), 143-163.

Goel, S., Perelman, M., Shroff, R., & Sklansky, D. A. (2017). Combatting police discrimination in the age of big data. *New Criminal Law Review*, *20*(2), 181-232.

Goetschel, M., & Peha, J. M. (2017). Police perceptions of body-worn cameras. *American Journal of Criminal Justice*, *42*(4), 698-726.

Groff, E. R., Ratcliffe, J. H., Haberman, C. P., Sorg, E. T., Joyce, N. M., & Taylor, R. B. (2015). Does what police do at hot spots matter? The Philadelphia policing tactics experiment. *Criminology*, *53*(1), 23-53.

Haberman, C. P., & Ratcliffe, J. H. (2012). The predictive policing challenges of near repeat armed street robberies. *Policing: a journal of policy and practice*, *6*(2), 151-166.

Han, J., Huang, Y., Liu, S., & Towey, K. (2020). Artificial intelligence for anti-money laundering: a review and extension. *Digital Finance*, *2*(3), 211-239.

Hedberg, E. C., Katz, C. M., & Choate, D. E. (2017). Body-worn cameras and citizen interactions with police officers: Estimating plausible effects given varying compliance levels. *Justice quarterly*, *34*(4), 627-651.

Henderson, S. E. (2017). A few criminal justice big data rules. *Ohio St. J. Crim. L.*, *15*, 527.

Henschke, A., Reed, A., Robbins, S., & Miller, S. (2021). *Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism*, Springer Nature.

Hert, P. de, & Papakonstantinou, V. (2016). The new police and criminal justice data protection directive: a first analysis. *New journal of European criminal law*, *7*(1), 7-19.

Hilbert, M. (2016). Big data for development: A review of promises and challenges. *Development Policy Review*, *34*(1), 135-174.

Hirose, M. (2017). Privacy in public spaces: The reasonable expectation of privacy against the dragnet use of facial recognition technology. *Connecticut Law Review*, *49*, 1591.

Hirsch Ballin, E.H. (2021) *Mensenrechten als ijkpunten van artificiële intelligentie*, WRR: Den Haag (Working Paper).

Hitchcock, A., Holmes, R., & Sundorph, E. (2017). Bobbies on the net: a police workforce for the digital age. *London: Reform*.

Hobson, Z., Yesberg, J. A., Bradford, B., & Jackson, J. (2021). Artificial fairness? Trust in algorithmic police decision-making. *Journal of experimental criminology*, 1-25.

Hood, J. (2020). Making the body electric: The politics of body-worn cameras and facial recognition in the United States. *Surveillance & Society*, *18*(2), 157-169.

Hung, T. W., & Yen, C. P. (2021). On the person-based predictive policing of AI. *Ethics and Information Technology*, *23*(3), 165-176.

Isaac, W. S. (2018). Hope, hype, and fear: the promise and potential pitfalls of artificial intelligence in criminal justice. *Ohio St. J. Crim. L.*, *15*, 543.

Jackson, R. D. (2020). "I Approved It… And I'll Do It Again": Robotic Policing and Its Potential for Increasing Excessive Force" in: *Societal Challenges in the Smart Society*, pp. 511-522.

Jennings, W. G., Lynch, M. D., & Fridell, L. A. (2015). Evaluating the impact of police officer body-worn cameras (BWCs) on response-to-resistance and serious external complaints: Evidence from the Orlando police department (OPD) experience utilizing a randomized controlled experiment. *Journal of criminal justice*, *43*(6), 480-486.

Joh E (2014) Policing by numbers: big data and the fourth amendment. Wash Law Rev 89:35–68.

Joh, E. E. (2016a). Policing police robots. *UCLA L. Rev. Discourse*, *64*, 516.

Joh, E. E. (2016b). The new surveillance discretion: automated suspicion, big data, and policing. *Harv. L. & Pol'y Rev.*, *10*, 15.

Joh, E. E. (2017). Artificial intelligence and policing: First questions. *Seattle UL Rev.*, *41*, 1139.

Joh, E. E. (2017). Feeding the machine: Policing, crime data, & algorithms. *Wm. & Mary Bill Rts. J.*, *26*, 287.

Joh, E.E. (2018a) Artificial Intelligence and Policing: First Questions" in: *Seattle University Law Review,* 41 (4), pp. 1139-1144.

Joh, E.E. (2018b) "Automated policing" in: *Ohio State Journal of Criminal Law,* Vol. 15, No. 2, pp. 559-564.

Joh, E. E. (2019a). Policing the smart city. *International Journal of Law in Context*, *15*(2), 177-182.

Joh, E. E. (2019b). The consequences of automating and deskilling the police. *UCLA L. Rev. Discourse*, *67*, 133.

Johnson, R. R., Sterling, L. S., Jiang, S., & Poole, S. D. (2018). Toledo Police Department Prolific Offender Surveillance and Apprehension Unit Smart Policing Initiative Final Report.

Karpinsky, N. D., Long, S. K., & Bliss, J. P. (2017, September). The relationship of the Penny Beliefs Weapons scale to robotic peacekeeper compliance and trust. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 61, No. 1, pp. 1580-1584). Sage CA: Los Angeles, CA: SAGE Publications.

Karppi, T., Boehlen, M., & Granata, Y. (2018). Killer Robots as cultural techniques. *International Journal of Cultural Studies*, *21*(2), 107-123.

Kasat, S., Tupe, K., Kshatriya, V., More, R., & Tambe, M. P. S. (2019). Recognition of Theft by Gestures using Kinect Sensor in: Machine Learning, Vol. 6, No. 11.

Katz, C. M., Choate, D. E., Ready, J. R., & Nuño, L. (2014). Evaluating the impact of officer worn body cameras in the Phoenix police department. *Phoenix, AZ: Center for Violence Prevention & Community Safety, Arizona State University*.

Kaufmann, M., Egbert, S., & Leese, M. (2019). Predictive policing and the politics of patterns. *The British Journal of Criminology*, *59*(3), 674-692.

Kaur, P., Kumar, Y., & Gupta, S. (2022). Artificial Intelligence Techniques for the Recognition of Multi-Plate Multi-vehicle Tracking Systems: A Systematic Review. *Archives of Computational Methods in Engineering*, 1-18.

Keenan, B. (2021). Automatic facial recognition and the intensification of police surveillance. *The Modern Law Review*, *84*(4), 886-897.

Kernaghan, K. (2014). The rights and wrongs of robotics: Ethics and robots in public organizations. *Canadian Public Administration*, *57*(4), 485-506.

Keyvanpour, M. R., Javideh, M., & Ebrahimi, M. R. (2011). Detecting and investigating crime by means of data mining: a general crime matching framework. *Procedia Computer Science*, *3*, 872-880.

Khalaf Al Mazrouei, F. (2022). Abu Dhabi Police… A Modern Vision that Keeps Pace with Development and Future Foreseeing. *Policing: A Journal of Policy and Practice*, *16*(2), 233-235.

Khorshidi, S., Carter, J. G., & Mohler, G. (2020, December). Repurposing recidivism models for forecasting police officer use of force. In *2020 IEEE International Conference on Big Data (Big Data)* (pp. 3199-3203). IEEE.

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and engineering ethics*, *26*(1), 89-120.

Kool, D. de, Vermeeren, B. & B. Steijn (2020a) *Kunstmatige Intelligentie bij de politie. Praktische en sociale lessen ten aanzien van het aangifteproces* Erasmus Universiteit Rotterdam ESSB/Risbo: Rotterdam.

Kool, D. de, Vermeeren, B. & B. Steijn (2020b) "Perceived Opportunities and Challenges of Artificial Intelligence within the Police. A Public Management Perspective" in: G. Jacobs, I. Suojajen, K. Horton & S. Bayerl (eds.), *International Security Management: New Solutions,* Springer, pp.343-356.

Kool, D. de, Vermeeren, B. & B. Steijn (2020c) "AI in het aangifteproces. Is er een fit?" in: *Tijdschrift voor de Politie*, nummer 5, pp. 32-36.

Kostka, G., Steinacker, L., & Meckel, M. (2021). Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. *Public Understanding of Science*, 09636625211001555.

Kotsoglou, K. N., & Oswald, M. (2020). The long arm of the algorithm? Automated Facial Recognition as evidence and trigger for police intervention. *Forensic Science International: Synergy*, *2*, 86-89.

Kouziokas, G. N. (2017). The application of artificial intelligence in public administration for forecasting high crime risk transportation areas in urban environment. *Transportation research procedia*, *24*, 467-473.

Kumar, D. L. B., Selvavinayagam, K., & Babu, S. S. (2014). Assessment of crime & its mapping using remote sensing & 3D Geo-spatial model for Chennai city. *Assessment*, *3*(3).

Kuo, P. F., & Lord, D. (2019). A promising example of smart policing: A cross-national study of the effectiveness of a data-driven approach to crime and traffic safety. *Case studies on Transport policy*, *7*(4), 761-771.

Kyriakidou, M., Sharkey, A., & Blades, M. (2013, March). Ethical dilemmas for children's robot crime interviewers. In *First UKRE workshop on robot ethics, University of Sheffield* (Vol. 25).

Lassila, S. (2021). *Designing the Trustworthy Principles of Artificial Intelligence: case: Finnish Police*, (master thesis Laurea University of Applied Sciences).

Levine, E. S., Tisch, J., Tasso, A., & Joy, M. (2017). The New York City police department's domain awareness system. *Interfaces*, *47*(1), 70-84.

Lin, P., Abney, K., & Bekey, G. (2011). Robot ethics: Mapping the issues for a mechanized world. *Artificial Intelligence*, *175*(5-6), 942-949.

Lin, R. (2016). Police body worn cameras and privacy: Retaining benefits while reducing public concerns. *Duke L. & Tech. Rev.*, *14*, 346.

Mac, T. T., Copot, C., Lin, C. Y., Hai, H. H., & Ionescu, C. M. (2020, March). Towards the development of a smart drone police: Illustration in traffic speed monitoring. In *Journal of Physics: Conference Series* (Vol. 1487, No. 1, p. 012029). IOP Publishing.

Macnish, K., Wright, D., & Jiya, T. (2020). Predictive policing in 2025: A scenario. In: H. Jahankhani e.a. (eds) *Policing in the Era of AI and Smart Societies* (pp. 199-215). Springer, Cham, pp. 199-215.

Macrorie, R., Marvin, S., & While, A. (2021). Robotics and automation in the city: a research agenda. *Urban Geography*, *42*(2), 197-217.

Mali, B., Bronkhorst-Giesen, C., & den Hengst, M. (2017). *Predictive policing: lessen voor de toekomst: een evaluatie van de landelijke pilot*, Politieacademie: Apeldoorn.

McDaniel, J., & Pease, K. (Eds.). (2021). *Predictive Policing and Artificial Intelligence*. Routledge.

McGarrell, E. F., Drake, G., Stephens, D., & Center, M. J. S. (2015). Smart Policing and the Michigan State Police.

Meghdari, A., & Alemi, M. (2018, August). Recent advances in social & cognitive robotics and imminent ethical challenges. In *Recent Advances in Social & Cognitive Robotics and Imminent Ethical Challenges (August 22, 2018). Proceedings of the 10th International RAIS Conference on Social Sciences and Humanities*.

Meijer, A., & Wessels, M. (2019). Predictive policing: Review of benefits and drawbacks. *International Journal of Public Administration*, *42*(12), 1031-1039.

Meijer, A., Lorenz, L., & Wessels, M. (2021). Algorithmization of bureaucratic organizations: Using a practice lens to study how context shapes predictive policing systems. *Public Administration Review*, *81*(5), 837-846.

Miller, K. (2014). Total surveillance, big data, and predictive crime technology: Privacy's perfect storm. *J. Tech. L. & Pol'y*, *19*, 105.

Milosevic, D., Subošić, D., Vasiljevic, P., Nikolic, V., & Markoski, B. (2020) Possibilities of Using Big Data Analytic in Police Work.

Ministerie van Economische Zaken en Klimaat (2019) *Strategisch Actieplan voor Artificiële Intelligentie* https://www.rijksoverheid.nl/documenten/beleidsnotas/2019/10/08/strategisch-actieplan-voor-artificiele-intelligentie

Mohler, G. O., Short, M. B., Malinowski, S., Johnson, M., Tita, G. E., Bertozzi, A. L., & Brantingham, P. J. (2015). Randomized controlled field trials of predictive policing. *Journal of the American statistical association*, *110*(512), 1399-1411.

Moon, H., Choi, H., Lee, J., & Lee, K. S. (2017). Attitudes in Korea toward introducing smart policing technologies: Differences between the general public and police officers. *Sustainability*, *9*(10), 1921.

Mrozla, T. (2021). Procedural and distributive justice: Effects on attitudes toward body-worn cameras. *International Journal of Police Science & Management*, *23*(3), 317-327.

Murphy, J. R. (2018). Chilling: The constitutional implications of body-worn cameras and facial recognition technology at public protests. *Wash. & Lee L. Rev. Online*, *75*, 1, pp….

Nakar, S., & Greenbaum, D. (2017). Now you see me: Now you still do: Facial recognition technology and the growing lack of privacy. *BUJ Sci. & Tech. L.*, *23*, 88.

Newell, B. C. (Ed.). (2020). *Police on Camera: Surveillance, Privacy, and Accountability*. Routledge.

Noriega, M. (2020). The application of artificial intelligence in police interrogations: An analysis addressing the proposed effect AI has on racial and gender bias, cooperation, and false confessions. *Futures*, *117*, 102510.

Norton, A. (2013). Proactive Policing in the Trinidad and Tobago Police Service (TTPS) using" Big Data". *International Journal of Computer Applications*, *72*(18).

Oswald, M., Grace, J., Urwin, S., & Barnes, G. C. (2018). Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental'proportionality. *Information & Communications Technology Law*, *27*(2), 223-250.

Pavone, V., & Esposti, S. D. (2012). Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. *Public Understanding of Science*, *21*(5), 556-572.

Pelzer, R. (2018). Policing of terrorism using data from social media. *European Journal for Security Research*, *3*(2), 163-179.

Perkowski, J. (2019). *A Big Data Approach to Examining Police Use of Force and Body-Worn Camera Implementation* (Doctoral dissertation, State University of New York at Stony Brook).

Perry, W. L. (e.a.) (2013) *Predictive policing: The role of crime forecasting in law enforcement operations*. Rand Corporation.

Petit, N. (2018). Artificial intelligence and automated law enforcement: A review paper. *Available at SSRN 3145133*.

Phippen, A., & Bond, E. (2020). Image Recognition in Child Sexual Exploitation Material—Capabilities, Ethics and Rights. In: H. Jahankhani e.a. (eds.) *Policing in the Era of AI and Smart Societies* (pp. 179-198). Springer, Cham, pp. 179-197).

Popova, M. (2020). Engaging the Artificial Intelligence in support of the Police Activity. *Knowledge International Journal*, *43*(5), 957-962.

Prabakar, M., & Kim, J. H. (2013, August). TeleBot: Design concept of telepresence robot for law enforcement. In *Proceedings of the 2013 World Congress on Advances in Nano, Biomechanics, Robotics, and Energy Research (ANBRE 2013), Seoul, Korea*.

Purshouse, J., & Campbell, L. (2019). Privacy, crime control and police use of automated facial recognition technology. *Criminal Law Review*, *2019*(3), 188-204.

Raaijmakers, S. (2019). Artificial intelligence for law enforcement: challenges and opportunities. *IEEE Security & Privacy*, *17*(5), 74-77.

Rademacher, T. (2020). Artificial intelligence and law enforcement. In: T. Wischmeyer &T. Rademacher (Eds) *Regulating artificial intelligence*, Springer, pp. 225-254.

Raponi, S., Oligeri, G. & Ali, I.M. Sound of guns: digital forensics of gun audio samples meets artificial intelligence. *Multimed Tools Appl* (2022). https://doi.org/10.1007/s11042-022-12612-w.

Ratcliffe, J. H., Grof, E. R., Haberman, C. P., Sorg, E. T., & Joyce, N. (2013). Philadelphia, Pennsylvania Smart Policing Initiative: Testing the impacts of differential police strategies on violent crime hotspots. *Washington: Bureau of Justice Assistance*.

Ratcliffe, J. (2015). What is the future… of predictive policing. *Practice*, *6*(2), 151-166.

Reid, M. (2017). Rethinking the Fourth Amendment in the Age of Supercomputers, Artificial Intelligence, and Robots. *W. Va. L. Rev.*, *119*, 863.

Reid, T., & Gibert, J. (2022). Inclusion in human–machine interactions. *Science*, *375*(6577), 149-150.

Richards N.M. (2013) The dangers of surveillance. Harv Law Rev 126:1934–1965.

Richards, N. M., & King, J. H. (2014). Big data ethics. *Wake Forest L. Rev.*, *49*, 393.

Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *NYUL Rev. Online*, *94*, 15.

Roach, S. C. (2016). Holding killer robots accountable? The new moral challenge of 21st century warfare. Columbia University Journal of International Affairs. https:// jia.sipa.columbia.edu/online-articles/holding-killer-robots-accountable.

Rodríguez-Jiménez, J. M. (2018, October). An approach for the police districting problem using artificial intelligence. In *International Symposium on Methodologies for Intelligent Systems* (pp. 141-150). Springer, Cham.

Royakkers, L., F. Daemen & R. van Est (2012) *Overal robots. Automatisering van de liefde tot de dood*, Boom Lemma Uitgevers: Den Haag.

Royakkers, L., & van Est, R. (2015). A literature review on new robotics: automation from love to war. *International journal of social robotics*, *7*(5), 549-570.

Rummens, A. (2021). *Predictive policing as a tool for crime prediction and prevention: A methodological and operational evaluation* (Doctoral dissertation, Ghent University).

Rushkin, S. (2013). The legislative response to mass police surveillance. *Brook. L. Rev.*, *79*, 1.

Sandhu, A., & Fussey, P. (2021). The 'uberization of policing'? How police negotiate and operationalise predictive policing technology. *Policing and Society*, *31*(1), 66-81.

Sappelli, M., de Boer, M. H., Smit, S. K., & Bomhof, F. (2017). A vision on Prescriptive Analytics. *ALLDATA 2017*, 54.

Saunders, J., Hunt, P., & Hollywood, J. S. (2016). Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot. *Journal of Experimental Criminology*, *12*(3), 347-371.

Schlossberg T (2015) New York police begin using ShotSpotter system to detect gunshots. *The New York Times.* https://www.nytimes.com/2015/03/17/nyregion/shotspotter-detection-system-pinpoints-gunshot-locations-and-sends-data-to-the-police.html.

Selbst, A. D. (2017). Disparate impact in big data policing. *Ga. L. Rev.*, *52*, 109.

Setyan, A. P., Affandi, A., Sumpeno, S., & Romahadi, D. (2021, June). Predicting Vehicle Theft with Backpropagation Algorithm in East Java Regional Police. In *2021 International Conference on Artificial Intelligence and Computer Science Technology (ICAICST)*, (pp. 19-24.

Shapiro, A. (2017). Reform predictive policing. *Nature news*, *541*(7638), 458.

Shapiro, A. (2019). Predictive policing for reform? Indeterminacy and intervention in big data policing. *Surveillance & Society*, *17*(3/4), pp. 456-472.

Shaw, I. (2017). Policing the future city: Robotic being-in-the-world. *AntipodeFoundation. org*, 19.

Sheehey, B. (2019). Algorithmic paranoia: the temporal governmentality of predictive policing. *Ethics and Information Technology*, *21*(1), pp. 49-58.

Cheema, A.P., S. Sharma, K. Nandankumar, M. R. Rahul and E. H. Rohit, "Self-Care, Interactive & Surveillance Robot," *2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, 2022, pp. 1-5, doi: 10.1109/ACCAI53970.2022.9752512.

Sheikha, D. A., Khalil, A., & Moreb, M. A. (n.d.) *Artificial Intelligence For Network Intrusion Detection And CyberCrimes*. Derar Abu Sheihka's Lab, Arab American University.

Simmons, R. (2016). Quantifying criminal procedure: how to unlock the potential of big data in our criminal justice system. *Mich. St. L. Rev.*, 947.

Sluis, A. van & S. van de Walle (2015) "The significance of police-citizen contacts for public trust in the police in the Netherlands" in: *EJPS,* Vol. 3, No. 1, pp. 78-98.

Smit, S. K., Vries, A. D., Kleij, R., & van Vliet, P. J. (2016). Van predictive naar prescriptive policing: Verder dan vakjes voorspellen, TNO.

Snijders, D., Biesiot, M., Munnichs, G., & van Est, R. (2019). *Burgers en sensoren: acht spelregels voor de inzet van sensoren voor veiligheid en leefbaarheid,* Rathenau Instituut: Den Haag.

Spithoven, R., & Beerends, S. (2019). Veiligheid uit de glazen bol? In: *Tijdschrift voor Veiligheid*, *18*, 3-4.

Stahl, B. C., & Wright, D. (2018). Ethics and privacy in AI and big data: Implementing responsible research and innovation. *IEEE Security & Privacy*, *16*(3), 26-33.

Sumantri, V. K. (2019). Legal responsibility on errors of the artificial intelligence-based robots. *Lentera Hukum*, *6*, 337.

Szocik, K., & Abylkasymova, R. (2021). Ethical Issues in Police Robots. The Case of Crowd Control Robots in a Pandemic. *Journal of Applied Security Research*, 1-16.

Tao, F., Akhtar, M. S., & Jiayuan, Z. (2021). The future of artificial intelligence in cybersecurity: a comprehensive survey. *EAI Endorsed Transactions on Creative Technologies*, e3.

Tasioulas, J. (2019). First steps towards an ethics of robots and artificial intelligence. *Journal of Practical Ethics*, *7*(1).

Tene, O., & Polonetsky, J. (2012). Big data for all: Privacy and user control in the age of analytics. *Nw. J. Tech. & Intell. Prop.*, *11*, xxvii.

Terpstra, J., & Salet, R. (2019). Change and continuity in the police: Introduction to the Special Issue. *International Journal of Police Science & Management*, *21*(4), 193-195.

Theodoridis, T., & Hu, H. (2012). Toward intelligent security robots: A survey. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, *42*(6), 1219-1230.

Thomasen, K., Dunn, S., Robertson, K., Hrick, P., Khoo, C., Kim, R., ... & Parsons, C. A. (2021). Submission to the Toronto Police Services Board's Use of New Artificial Intelligence Technologies Policy-LEAF and The Citizen Lab. *Available at SSRN 3989271*.

Turner, J. (2018). *Robot rules: Regulating artificial intelligence*. Palgrave Macmillan.

U.N.I.C.R.I (2019) *Artificial Intelligence and Robotics for Law Enforcement.*

U.N.I.C.R.I. (2020) *Special Collection on AI in Criminal Justice*.

Verhage, A., & Boels, D. (2015) "Systematische reviews van kwalitatief onderzoek binnen de criminology" in: *Panopticon*, *36*(3), pp. 302-311.

Vermeulen, I., Soudijn, M., & van der Leest, W. (2021). Open heimelijke netwerken in de Nederlandstalige georganiseerde synthetische drugscriminaliteit. *Tijdschrift voor Criminologie*, *63*(2).

Visker, O. (2019). *Modern Scotland Yard: Improving surveillance policies using adversarial agent based modelling and reinforcement learning* (Doctoral dissertation). Universiteit van Groningen Interpol

Voigt, R., Camp, N. P., Prabhakaran, V., Hamilton, W. L., Hetey, R. C., Griffiths, C. M., ... & Eberhardt, J. L. (2017). Language from police body camera footage shows racial disparities in officer respect. *Proceedings of the National Academy of Sciences*, *114*(25), 6521-6526.

Waardenburg, M., Groenleer, M., de Jong, J., & Bolhaar, H. (2018). Evidence-based prevention of organized crime: Assessing a new collaborative approach. *Public Administration Review*, *78*(2), 315-317.

Waardenburg, L., Sergeeva, A. V., & Huysman, M. (2020). Predictive policing ontcijferd: Een etnografie van het'Criminaliteits Anticipatie Systeem'in de praktijk. In *Informatiegestuurde politie* (pp. 69-88). Gompel & Svacina.

Waardenburg, L., Huysman, M., & Agterberg, M. (2021). Hoe kan artificial intelligence (AI) SLIM worden gemanaged?. *Holland Management Review*, *195*, 25-30.

Walsh, D., & Downe, S. (2006) "Appraising the quality of qualitative research" in: *Midwifery*, *22*(2), pp. 108-119.

Wanebo, T. (2018). Remote killing and the Fourth Amendment: Updating Constitutional law to address expanded police lethality in the robotic age. *UCLA L. Rev.*, *65*, 976.

Welsh, B. C., & Rocque, M. (2014). When crime prevention harms: A review of systematic reviews. *Journal of Experimental Criminology*, *10*(3), 245-266.

Went, R., M. Kremer & A. Knotterus (2015) *De robot de baas. De toekomst van werk in het tweede machinetijdperk*, WRR: Den Haag.

White, M. D., & Katz, C. M. (2013). Policing convenience store crime: Lessons from the Glendale, Arizona smart policing initiative. *Police Quarterly*, *16*(3), 305-322.

Willems, D., & Doeleman, R. (2014). Predictive Policing–wens of werkelijkheid?. *Het Tijdschrift voor de Politie*, *76*(4), 5.

Williams, M. L., Burnap, P., & Sloan, L. (2017). Crime sensing with big data: The affordances and limitations of using open-source communications to estimate crime patterns. *The British Journal of Criminology*, *57*(2), 320-340.

Wisskirchen, G. e.a. (2017) *Artificial Intelligence and Robotics and Their Impact on the Workplace,* IBA Global Employment Institute.

Wolfe, S. E., Rojek, J., Kaminski, R., & Nix, J. (2015). City of Columbia (SC) Police Department Smart Policing Initiative Final Report.

Wood, G. N. (2020). The problem with killer robots. Journal of Military Ethics, 19(3), 220-240.

Yalcin, G., Themeli, E., Stamhuis, E. *et al.* Perceptions of Justice By Algorithms. *Artif Intell Law* (2022). https://doi.org/10.1007/s10506-022-09312-z.

Yokum, D., Ravishankar, A., & Coppock, A. (2017). Evaluating the effects of police body-worn cameras. *Washington, DC: The Lab@ DC*, *20*.

Xiong, J. (2017, May). Use Big Data Thinking in the Cultivation of Police Intelligence Ability. In *2017 International Conference on Applied Mathematics, Modelling and Statistics Application (AMMSA 2017)* (pp. 57-60). Atlantis Press.

Zeng, Y., Lu, E., Sun, Y., & Tian, R. (2019). Responsible facial recognition and beyond. *arXiv preprint arXiv:1909.12935*.

Bijlage 1: Geraadpleegde experts

- Prof.dr Jeffrey Brantingham
- Dr Anneleen Rummens
- Prof. dr Elizabeth Joh
- Prof. dr Randy Goebel

- Lindeberg Pessoa Leite
- Prof. dr Stefano Puntoni
- Dr Katharina Bauer
- Dr Bas Testerink

Bijlage 2: Deelnemers focusgroep

- Riwish Hoeseini
- Matthijs Flim
- Sara Jahfari
- Gerard Kuijlaars
- Linda Li
- Oscar Wijsman

Bijlage 3: Leden van de begeleidingscommissie

- Dr. Ana Barros
- Prof. Dr. Floris Bex
- Drs. Katinka Knops
- Drs. Kirsti Schuiling
- Drs. Annemieke Venderbosch

Bijlage 4: Topic list interviews met experts

Inleiding

In dit interview staat de volgende concrete toepassing (casus) centraal.

Kansen

Wat zijn de kansen van de concrete toepassing (casus) voor de politie?

Risico's

Wat zijn de risico's van de concrete toepassing (casus) voor de politie?

Concrete ervaringen

Welke concrete (positieve of negatieve) ervaringen heeft de politie met de concrete toepassing (casus) opgedaan?

Kritische succesfactoren

Wat zijn de kritische succesfactoren om de concrete toepassing (casus) effectief toe te passen door de politie?

Concrete lessen en aandachtspunten

Welke concrete lessen kan de (Nederlandse) politie trekken uit de opgedane ervaringen?

Overige inzichten

Zijn er nog andere relevante inzichten om te delen?