Dit is het geaccepteerde manuscript van een boekhoofdstuk. Graag als volgt naar dit werk te verwijzen:
Landman, W. (2024). Politiewerk en digitale technologie, in: E.R. Muller, N. Kop & E.J. van der Torre (red.), *Politie. Organisatie en functioneren van de politie in Nederland (4de druk)*. Deventer: Wolters Kluwer, 307-333.

Hoofdstuk 15

Politie en digitale technologie

W. Landman

15.1.Inleiding

15.1.1. Technologie en politie

Sinds het ontstaan van de politie wordt het politiewerk beïnvloed door technologische ontwikkelingen in de samenleving. Deze invloed verloopt langs twee lijnen. Technologie heeft in de eerste plaats invloed op de aard van de criminaliteit en onveiligheid in de samenleving. Door het gebruik van technologie in de samenleving ontstaan er nieuwe risico's en fenomenen op het gebied van criminaliteit en onveiligheid. De ontwikkeling van de auto heeft bijvoorbeeld tot nieuwe vormen van verkeersonveiligheid in de samenleving geleid. De opkomst van informatie- en communicatietechnologie in de samenleving heeft geresulteerd in digitalisering van criminaliteit. De politie moet zich aan veranderingen in de aard van de criminaliteit en onveiligheid aanpassen en wordt op deze wijze beïnvloed door technologie.

Technologie wordt daarnaast door de politie gebruikt met de intentie om het politiewerk te verbeteren of moderniseren. De wijze waarop de noodhulp op dit moment wordt uitgevoerd, is bijvoorbeeld een uitvloeisel van onder andere de ontwikkeling van de politieauto en van informatie- en communicatietechnologie. In dit hoofdstuk staat deze invalshoek centraal: de inzet en het gebruik van technologie door de politie. Technologie is een breed begrip. Wat onder 'technologie' wordt verstaan, is afhankelijk van verschillende factoren, waaronder het tijdsperspectief.[1] In de huidige samenleving heeft technologie vooral de betekenis van digitale technologie: technologie die met behulp van microprocessoren (computers) gegevens genereert, opslaat en verwerkt. Dit hoofdstuk gaat in op het gebruik van digitale technologie door de politie en de consequenties van dit gebruik.

15.1.2. Opbouw van dit hoofdstuk

De volgende paragraaf gaat in op digitale technologie in de samenleving. In deze paragraaf komen de belangrijkste ontwikkelingen en begrippen met betrekking tot digitale technologie aan de orde. In paragraaf 3 staat het gebruik van digitale technologie door de politie centraal. In deze paragraaf worden verschillende toepassingen van digitale technologie door de politie beschreven. Deze toepassingen zijn 'temporeel' geordend: het begint met toepassingen die (hoofdzakelijk) worden gebruikt voor terugkijken en eindigt met toepassingen waarmee wordt beoogd vooruit te kijken. Het is geen uitputtend overzicht, maar biedt wel inzicht in de ontwikkelingen die binnen de politie in Nederland gaande zijn. Paragraaf 4 behandelt de gevolgen van de inzet en gebruik van technologie voor de politiefunctie, politieorganisatie en

[1] Lauwaert 2021.

het politievakmanschap. Dit is een beschrijving op hoofdlijnen. Paragraaf 5 verplaatst het perspectief naar de samenleving: hoe beïnvloedt de inzet en het gebruik van digitale technologie publieke waarden, waaronder effectiviteit, privacy en gelijke behandeling? In paragraaf 6 wordt het hoofdstuk afgesloten met een korte slotbeschouwing.

15.2.Digitale technologie en samenleving

15.2.1. Digitalisering en dataficatie

Het fundament van de digitale revolutie die zich sinds de jaren ’70 van de vorige eeuw heeft voltrekken, was de introductie van de microprocessor of microchip van Intel.[2] Dit legde de basis voor de komst van Personal Computer (PC) in de jaren ‘80. In de jaren ’90 volgde de ontwikkeling van het internet. Losstaande netwerken van computers konden door middel van een protocol met elkaar worden verbonden. Als gevolg hiervan is een wereldwijd netwerk ontstaan: het internet. Na de millenniumwisseling ontwikkelde het internet zich van een passief, informatie gevend medium – ook wel aangeduid als Web 1.0 – naar een interactief medium waaraan gebruikers op allerlei manieren kunnen bijdragen: Web 2.0.[3] In ongeveer dezelfde periode kwam de smartphone op de markt: de mobiele telefoon werd vanaf dat moment een computer die is verbonden met het internet en waarop gebruikers allerlei applicaties kunnen installeren en gebruiken, waaronder apps van sociale mediaplatformen.

In de afgelopen jaren zijn er aan steeds meer apparaten microchips toegevoegd.[4] Hierbij kan worden gedacht aan allerlei apparaten voor het menselijk lichaam (zoals horloges), het huis (zoals deurbellen), mobiliteit (zoals auto’s) en de leefomgeving (zoals straatverlichting). Deze apparaten zijn in toenemende mate met het internet verbonden. Dit netwerk van onderling verbonden apparaten wordt ook wel het *Internet of Things* (IoT) genoemd. Het Internet of Things zal naar verwachting een steeds grotere impact hebben op onze samenleving en zal rond 2030 niet meer weg te denken zijn uit ons dagelijks leven. De overgang naar de vijfde generatie mobiele netwerken (5G) speelt hierbij een belangrijke rol, omdat hierdoor de snelheid en betrouwbaarheid van draadloze verbindingen wordt verbeterd. Dit is nodig, omdat de communicatie – data-uitwisseling – tussen apparaten veel van het mobiele netwerk vraagt.

De voortschrijdende digitalisering heeft onder andere als gevolg dat steeds meer menselijke handelingen resulteren in digitale data. De meeste activiteiten en interacties van mensen die leven in een gedigitaliseerde samenleving genereren data:[5] welke boodschappen we doen, waar we lopen en rijden, wat we lezen, wat we kijken, met wie we bellen, energieverbruik, resultaten op school, prestaties op werk en ga zo maar door.[6] De digitale data die door menselijke handelingen worden geproduceerd, worden vervolgens in andere processen gebruikt, zoals het op maat maken van advertenties en doen van aanbevelingen op bijvoorbeeld LinkedIn of Netflix. Dit proces wordt dataficatie genoemd.

15.2.2. Algoritmen en artificiële intelligentie

In vrijwel alle digitale technologieën die nu opkomen, wordt gebruik gemaakt van algoritmen om grote hoeveelheden data te verwerken en hier inzichten en acties uit te genereren. Een

[2] Barrico 2019.
[3] Sadin 2021.
[4] Stephenson 2018.
[5] Beaulieu & Leonelli 2022.
[6] Buitenweg 2021.

algoritme is een set aan instructies die in programmeertaal zijn vastgelegd, zodat een computer deze kan opvolgen.[7] Inputdata worden via een geautomatiseerde reeks stappen omgezet in outputdata.

> Neem als voorbeeld een algoritme voor het voorspellen van woninginbraken. Een simpel algoritme is: het aantal te verwachten woninginbraken in dit gebied is 0,257 keer de maximumtemperatuur, plus 1,56 keer het aantal inbraken vorige week, minus 0,46 keer het aantal inbraken normaal op een maandag, plus 0,12 keer het aantal inbraken in een aanliggend gebied vorige week.[8]

Er zijn op hoofdlijnen twee verschijningsvormen van algoritmen.[9] De eerste verschijningsvorm is een op regels gebaseerd algoritme, ook wel een model-gedreven algoritme genoemd. De instructies worden in dit geval opgesteld door de mens en zijn veelal gebaseerd op een vorm van theorie. De tweede verschijningsvorm is een data-gedreven algoritme. Dit wil zeggen dat de computer op basis van data zelf komt tot instructies voor de stap van inputdata naar outputdata. De computer leert dan van de data. Om die reden wordt dit ook wel een machine learning algoritme genoemd.

> Neem als voorbeeld het voorspellen van recidive. Een model-gedreven algoritme wil zeggen dat je op basis van theorie factoren bepaalt, die van invloed zijn op recidive, en deze factoren een bepaalde zwaarte geeft. Als je vervolgens gegevens over iemand die is veroordeeld 'aan' de computer geeft, dan berekent het algoritme de kans op recidive. Een data-gedreven (machine learning) algoritme wil zeggen dat de computer (software) een grote hoeveelheid historische gevallen krijgt van veroordeelde personen die wel en niet zijn gerecidiveerd.[10] De computer identificeert op basis van deze trainingsdata verbanden tussen allerlei kenmerken van personen en omstandigheden én de uitkomst (wel/geen recidive). Op basis hiervan wordt door de computer een algoritme ontwikkeld dat recidive voorspelt. Dit algoritme is veel complexer dan het model-gedreven algoritme, omdat er tal van patronen worden gevonden die worden gebruikt voor het verwerken van de inputdata. Het gaat om honderden of soms zelfs duizenden rekenstapjes.[11] Door het algoritme voortdurend nieuwe, actuele gevallen van wel en geen recidive te geven, past het algoritme zich aan op de actualiteit. Een machine learning algoritme is dus adaptief.

De combinatie van toegenomen rekenkracht van microchips, de groeiende hoeveelheid data én de ontwikkeling van machine learning heeft als gevolg gehad dat in de afgelopen tien jaar een nieuwe systeemtechnologie is opgekomen: artificiële intelligentie. Artificiële intelligentie is geen afgebakende technologie, maar eerder een verzameling van technologieën die met elkaar gemeen hebben dat ze computers en andere apparaten in staat stellen om zich intelligent te gedragen. Artificiële intelligentie is uitgegroeid tot een van de grootste technologische innovaties van de digitale revolutie. De betekenis van artificiële intelligentie in de eenentwintigste eeuw is volgens de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) te vergelijken met die van elektriciteit in de negentiende eeuw en de verbrandingsmotor in de twintigste eeuw.[12]

---

[7] Koolstra, de Veer & Veltman 2021.
[8] Smit, de Vries & van der Vliet 2016.
[9] Fry 2018.
[10] Bex & Prakken 2020.
[11] Koolstra, De Veer & Veltman 2021.
[12] Wetenschappelijke Raad voor het Regeringsbeleid 2021.

Artificiële intelligentie heeft onder andere gevolgen voor de wijze waarop werk in organisaties wordt uitgevoerd.[13] Taken die voorheen door mensen werden uitgevoerd, worden in de eerste plaats geautomatiseerd. Dit betreft vooralsnog vooral afgebakende taken, zoals het analyseren van data om de ontwikkeling van de aandelenkoersen te voorspellen en op basis daarvan te handelen.[14] Artificiële intelligentie is bovenmenselijk goed in het uitvoeren van dit soort 'smalle' taken. Artificiële wordt daarnaast ingezet voor het versterken of aanvullen van menselijke vermogens en vaardigheden. Hierbij kan onder andere worden gedacht aan het ondersteunen van artsen bij diagnoses. Bij de impact van artificiële intelligentie op organisaties moet worden beseft dat de technologie nog in de kinderschoenen staat. Er zal in de komende jaren nog veel ontwikkeling plaatsvinden waarbij het steeds beter benaderen van de menselijke intelligentie centraal staat.[15]

15.3.Digitale technologie en politiewerk

15.3.1. Cryptocommunicatiedata

Criminelen gebruiken technologie voor verschillende doeleinden. Een van deze doeleinden is het afschermen van communicatie.[16] Dit vindt in de huidige informatiesamenleving onder andere plaats door versleutelde communicatie. Via zogenaamde ge-encrypte telefoons en een gesloten netwerk proberen criminelen om het risico op interceptie door opsporingsinstanties te minimaliseren. Het risico op interceptie blijft echter aanwezig. Tussen 2016 en 2023 zijn er door de politie in Nederland – al dan niet in samenwerking politiekorpsen uit andere landen – diverse 'cryptotelefoon-operaties' uitgevoerd waarmee de communicatie tussen criminelen is onderschept. Het gaat dan om Ennetcom (2017), PGP-safe (2017), IronChat (2018), EncroChat (2020), SkyECC (2021), ANOM (2021) en Exclu (2023).[17]

Deze operaties verschillen in termen van onder andere de betrokken diensten, de omvang van de operatie en interceptie én de wijze waarop het berichtenverkeer tussen criminelen is verkregen. De meest omvangrijke operaties vanuit Nederlands perspectief zijn EncroChat en Sky ECC. In deze (internationale) operaties zijn er opsporingsonderzoeken gestart naar de aanbieders van de versleutelde communicatie. In deze opsporingsonderzoeken is met behulp van interceptiesoftware de inhoudelijke communicatie en metadata – zoals locatiegegevens – van alle gebruikers onderschept. Het Team High Tech Crime (THTC) van de politie in Nederland heeft in de ontwikkeling van deze software een belangrijke rol gespeeld. Er is bij beide operaties enige tijd live meegekeken met het berichtenverkeer en daarnaast is het historische berichtenverkeer veilig gesteld. Het gaat in zijn totaliteit om meer dan 100 miljoen berichten van gebruikers van EncroChat en Sky ECC, die relevant zijn voor Nederland.

Het live meelezen met de versleutelde berichten die (zware) criminelen elkaar stuurden, was – mede gegeven de schaal waarop dit plaatsvond – een unieke gebeurtenis in de opsporing. Tijdens de livefase ontstond de vraag hoe ervoor kon worden gezorgd dat de meest relevante communicatie onder ogen van opsporingsambtenaren kwam, zodat er kon worden gereageerd op dreigende situaties, waaronder op handen zijnde liquidaties.

> Door het Nederlands Forensisch Instituut is tijdens de EncroChat operatie een model ontwikkeld waarmee kan worden voorspeld welke berichten uit de data een serieuze

[13] Waardenburg, Huysman & Agterberg 2020.
[14] Zie bijvoorbeeld Yang 2020.
[15] Wetenschappelijke Raad voor het Regeringsbeleid 2021.
[16] Kassab & Rosen 2019; Kruisbergen, Leukfeldt, Kleemans & Roks 2018.
[17] Zie de website van Jan-Jaap Oerlemans voor een overzicht van deze cryptophone-operaties.

bedreiging bevatten. Het model maakt gebruik van machine learning. Medewerkers van het instituut hebben met rechercheurs woordenlijsten met signaalwoorden gemaakt. Dat zijn woorden die criminele kunnen gebruiken om te wensen of te organiseren dat iemand wordt mishandeld, ontvoerd of vermoord. Denk aan: 'dood', 'slapen', 'poppen', 'afknallen' en 'verdwijnen'. De berichten die op basis hiervan naar voren kwamen, zijn vervolgens door rechercheurs beoordeeld met 'bedreigend' of 'niet bedreigend'. Dit was de basis om het model te leren om uit de context af te leiden of het daadwerkelijk om een bedreiging gaat. Het woord 'slapen' kan immers op verschillende manieren worden gebruikt. Op basis hiervan is het model getraind – met tienduizenden bedreigende en niet-bedreigende zinnen – door medewerkers van het Nederlands Forensisch Instituut. De politie heeft het model vervolgens ingezet en de resultaten gecontroleerd (feedback aan het model). Zo werd de software steeds intelligenter. Het model geeft ieder bericht een cijfer tussen de 0 en de 1 mee. Hoe dichter bij de 1, hoe groter de kans dat het om een bedreigend bericht gaat. Het model is in gebruik genomen door het Threat To Life team van de landelijke eenheid van de politie. Dit team heeft met de software berichten doorzocht. Tientallen personen zijn op basis hiervan door de politie gewaarschuwd vanwege een bedreiging voor hun leven.

De cryptotelefoon-operaties hebben, naast het live meelezen, geleid tot een enorme hoeveelheid data over de georganiseerde (drugs)criminaliteit die heeft plaatsgevonden. Om deze data te kunnen benutten, zijn er in de eenheden analyseteams ingericht onder regie van een landelijk analyseteam. In deze teams worden de data – met behulp van geavanceerde software – geanalyseerd. Relevante data zijn – door middel van juridische procedures – ter beschikking gesteld aan lopende opsporingsonderzoeken en zijn en worden gebruikt om nieuwe opsporingsonderzoeken te starten. Dit heeft gezorgd voor het omdraaien van de vanzelfsprekende volgorde in de opsporing van georganiseerde (drugs)criminaliteit: van 'zaak zoekt bewijs' naar 'bewijs zoekt zaak'.[18] Voorheen had de recherche – op basis van een signaal – een verdachte in beeld en werd met inzet van allerlei opsporingsmethoden geprobeerd om voldoende bewijsmiddelen voor vervolging te verkrijgen. Nu bevat het berichtenverkeer bewijs, maar is de identiteit van de verdachte nog niet bekend, omdat er in het berichtenverkeer gebruik wordt gemaakt van bijnamen. Het opsporingsonderzoek is vooral gericht op het identificeren van de verdachte(n) en het analyseren van het berichtenverkeer teneinde er bewijs uit te halen voor het dossier. Er hoeven niet of nauwelijks opsporingsmethoden te worden ingezet om aanvullende gegevens te verzamelen.

15.3.2. Digitaal-forensisch onderzoek en zaaksanalyse

Mede als gevolg van de dataficatie in de samenleving is de omvang van en varieteit in gegevens in opsporingsonderzoek sterk – zo niet exponentieel – toegenomen.[19] Burgers laten steeds meer digitale sporen achter die kunnen worden gebruikt in opsporingsonderzoek. Door inbeslagname of het hacken van geautomatiseerde werken of (grote) digitale gegevensdragers komen digitale gegevens steeds vaker in bulk bij de politie terecht.[20] Het gaat dan om omvangrijke datasets die op meerdere personen betrekking hebben. Bij bulkgegevens kan onder andere worden gedacht aan de hiervoor genoemde cryptocommunicatiedata. Het veiligstellen van omvangrijke datasets stelt de opsporing voor een uitdaging, omdat het niet uitvoerbaar is om deze handmatig te doorzoeken.[21] De politie maakt daarom in toenemende

[18] Tops 2022.
[19] Roest 2023.
[20] Fedorova et al. 2022.
[21] Te Molder 2022.

mate gebruik van digitaal forensische zoekmachines waarmee men in staat is te zoeken in omvangrijke datasets. Op zoek naar de spreekwoordelijke speld in de hooiberg.

> Een voorbeeld van digitaal forensische zoekmachine is het platform Hansken dat vanaf 2015 door het Nederlands Forensisch Instituut is ontwikkeld. Het doel van het platform is om digitale data snel en effectief te doorzoeken en zo bij te dragen aan het opsporen van strafbare feiten. Digitale data – waaronder foto's, bezochte internetpagina's, berichtenverkeer en mailverkeer – worden ingelezen, opgeslagen en geïndexeerd. De gebruiker kan vervolgens in de data zoeken op basis van onder andere trefwoorden en eigenschappen van sporen. De geselecteerde data kunnen worden weergegeven op een tijdlijn, bijvoorbeeld in geval van emailverkeer of chatgesprekken. Op het platform worden in toenemende mate tools ontwikkeld die gebruik van machine learning. Een voorbeeld hiervan is FIRE: forensic image recognition engine. FIRE is een machine learning algoritme voor forensisch fotomateriaal. Het algoritme kan afbeeldingen op foto's herkennen, bijvoorbeeld zeecontainers, bankpassen, vuurwapens, wiet en harddrugs, evenals teksten op afbeeldingen (zoals persoonsgegevens op rijbewijzen). Rechercheurs kunnen hiermee in een dataset zoeken naar een bepaalde categorie afbeeldingen.

Naast digitaal forensische zoekmachines wordt er door de politie gebruik gemaakt van analysetechnologieën waarmee verbanden tussen grote hoeveelheden data kunnen worden gelegd. In 2019 is in alle eenheden de Raffinaderij geïmplementeerd.[22] Deze voorziening is ontstaan gedurende het opsporingsonderzoek naar het netwerk van Robert M., de hoofdverdachte in de zogenaamde 'Amsterdamse zedenzaak'. In dit onderzoek was er behoefte aan technologie om rechercheurs en analisten in staat te stellen om met grote hoeveelheden data te werken. In de Raffinaderij kunnen data uit uiteenlopende bronnen – zoals basisinformatiesystemen, gegevensdragers, telefoontaps, bakens, internetdata en ANPR-camera's – worden ontsloten, geanalyseerd en gevisualiseerd. Ongestructureerde data worden gestructureerd waardoor deze geautomatiseerd kunnen worden geanalyseerd. Dit maakt het mogelijk om in een vroeg stadium verbanden te ontdekken tussen schijnbaar niet-gerelateerde gebeurtenissen, zowel binnen opsporingsonderzoeken als tussen opsporingsonderzoeken. De Raffinaderij heeft hiermee voor een doorbraak in de opsporing gezorgd.[23]

15.3.3. Slimme camera's en drones

De politie zet digitale technologieën in voor toezicht of surveillance in de publieke ruimte. Dit betreft in de eerste plaats het gebruik van slimme camera's. Dit gebruik is gestart met ANPR-camera's in 2004. ANPR staat voor *automatic number plate recognition*: het gaat om een camera die automatisch een kenteken kan herkennen. ANPR-camera's werken op basis van algoritmen die een beeld omzetten in een gelezen kenteken. Een geregistreerd kenteken wordt op twee manieren gebruikt. Het wordt in de eerste plaats vergeleken met kentekens die op referentielijsten staan, omdat ze worden gezocht. Daarnaast worden (alle) ingelezen kentekens voor een periode van 28 dagen opgeslagen ten behoeve van eventuele opsporingsdoeleinden.

Een ANPR-camera is een eenvoudige variant van een slimme camera. Een volgende generatie slimme camera's is in staat om bepaalde gedragingen te herkennen. De software van deze camera's wordt net zo lang getraind met data totdat zij in staat zijn om op basis van videobeelden bepaald gedrag te identificeren. Een voorbeeld van een dergelijke camera is de MONOcam.

---

[22] Ter Veen & Kop 2021.
[23] Klerks & Vink-Teeven 2020.

> In juli 2021 bracht de politie het bericht naar buiten dat zij slimme camera's gaat inzetten tegen afleiding in het verkeer. Met afleiding wordt bedoeld: bestuurders die een mobiele telefoon in hun handen hebben. De slimme camera heet de MONOcam en is grotendeels door de politie zelf ontwikkeld. De software is getraind op het herkennen van bestuurders die een apparaat in handen hebben. Zo heeft de software geleerd wanneer er sprake is van een overtreding. Als de software constateert dat iemand achter het stuur mogelijk een telefoon in de hand heeft, dan resulteert dit in een 'hit' die wordt doorgegeven aan een agent van het Team Verkeer. De agent beoordeelt of de bestuurder inderdaad een mobiele telefoon in diens hand heeft tijdens het rijden. Vervolgens wordt er (onafhankelijk van de eerste controle) een controle uitgevoerd door een tweede politieambtenaar. Als er sprake is van een overtreding, dan verstuurt de verbalisant de gegevens door naar het Centraal Justitieel Incassobureau (CJIB), dat vervolgens de bekeuring verstuurd. Volgens het Openbaar Ministerie leidt het gebruik van de MONOcam tot een pakkans van 95%.

Een andere verschijningsvorm van een slimme camera heeft betrekking op gezichtsherkenning. In Nederland wordt een systeem (CATCH) gebruikt waarmee foto's van onbekende verdachten worden vergeleken met een database waarin zo'n 1,3 miljoen foto's van veroordeelde en aangehouden personen zijn opgenomen. De politie in Nederland is bezig met een bredere inzet van gezichtsherkenningstechnologie in het kader van opsporing en mogelijk ook openbare orde en hulpverlening. Dit betreft real-time gezichtsherkenning in de publieke ruimte: camera's registreren dan de gezichten van passerende burgers en deze gezichtstemplates worden vergeleken met gezichtstemplates uit een database. De politie mag vooralsnog geen operationeel gebruik maken van deze vorm van gezichtsherkenning. In 2023 heeft de politie echter een kader voor de inzet van gezichtsherkenningstechnologie gepubliceerd waarmee wordt beoogd om inzet mogelijk te maken voor goed uitgedachte en welomlijnde gevallen, in het bijzonder ten behoeve van de opsporing.[24]

Slimme camera's hangen niet alleen in de publieke ruimte of zijn op politieauto's gemonteerd, maar zijn ook steeds vaker onderdeel van onbemande luchtvaartuigen: drones. De technologie van drones is oorspronkelijk ontwikkeld voor militaire doeleinden. Overheden zijn drones echter ook in toenemende mate in het civiele domein gaan gebruiken, onder andere voor politiewerk. De politie in Nederland zet sinds eind 2009 drones in voor de taakuitvoering. Dit waren eerst drones van Defensie op basis van een bijstandsaanvraag. Sinds 2018-2019 heeft de politie steeds meer eigen drones, die vooral worden ingezet voor toezicht en handhaving. Hierbij kan worden gedacht aan het volgen van voer- en vaartuigen, het monitoren van publiek tijdens grote evenementen, het verkrijgen van overzicht van een incident of plaats delict of het zoeken van vermiste personen. De ontwikkelingen op het gebied van drones gaan snel. Drones worden steeds autonomer. De politie experimenteert sinds 2022 met drones die automatisch naar de locatie van een incident kunnen vliegen. De videobeelden die worden gemaakt, worden doorgestuurd naar het Operationeel Centrum, die deze kan gebruiken voor de aansturing van de operatie. Er wordt daarnaast geëxperimenteerd met het gebruik van andere sensoren op drones, zoals sensoren die kunnen meten of er sprake is van een productielocatie voor synthetische drugs of het dumpen van drugsafval.

15.3.4. Online gegevensvergaring

De ontwikkeling van het internet in het algemeen en sociale media in het bijzonder heeft ertoe geleid dat burgers in Nederland steeds meer tijd online zijn. Dit heeft als gevolg dat vooral op

[24] Politie 2023.

sociale mediaplatformen informatie aanwezig is, die inzicht geeft in de handel en wandel van burgers. Deze online gegevens kunnen relevant zijn voor het politiewerk. De politie is in de afgelopen jaren dan ook steeds meer gaan investeren in online gegevensvergaring.[25]

Er worden in de eerste plaats online gegevens vergaard ten behoeve van intelligence, ook wel sturingsinformatie genoemd. Deze online monitoring vervult bijvoorbeeld een belangrijke rol bij het tegengaan van extremisme en radicalisering én het tijdig signaleren van mogelijke verstoringen van de openbare orde. In het kader van online monitoring maakt de politie gebruik van geavanceerde software die met behulp van artificiële intelligentie het internet en sociale media kan scannen. Dankzij slimme algoritmen is het mogelijk om in een gigantische stroom aan data te filteren en er voor de politie relevante berichten uit te pikken.

Online gegevensvergaring wordt ook ingezet ten behoeve van de opsporing. In het kader van de opsporing kan de politie – op basis van (bijzondere) opsporingsbevoegdheden – stelselmatiger online gegevens over verdachten verzamelen én tevens heimelijk opereren. Hierbij wordt ook gebruik gemaakt van geavanceerde software waarmee online gegevens over burgers kunnen worden vergaard, gecombineerd en geanalyseerd. Andere toepassingen van online gegevensvergaring voor opsporingsdoeleinden hebben bijvoorbeeld betrekking op het gebruik van software voor het monitoren van transacties met cryptovaluta. Dergelijke software wordt onder andere ingezet voor het onderzoeken van ransomware betalingen, die vaak plaatsvinden met cryptovaluta en in het bijzonder bitcoin.

15.3.5. Real-time intelligence

De data die voortkomen uit camera's, andere sensoren en online monitoring worden in toenemende mate bij elkaar gebracht ten behoeve van real-time intelligence: inzicht in actuele gebeurtenissen en dreigingen op basis waarvan het politiewerk kan worden aangestuurd. Zo heeft de politie in 2023 de beschikking gekregen over een sensingvoorziening waarmee op real-time basis datastromen uit verschillende toepassingen – te beginnen met ANPR-camera's – kunnen worden verzameld en verwerkt. De aansturing van het politiewerk vindt plaats door het operationeel centrum (OC) van de politie en wordt ondersteund door een daaraan gekoppeld centrum: het real-time intelligence center (RTIC). In het operationeel centrum van de politie wordt steeds meer gebruik gemaakt van slimme software die medewerkers in hun werk ondersteunt. Hierbij kan onder andere worden gedacht aan een applicatie die mogelijke vluchtroutes van daders in kaart brengt, bijvoorbeeld bij ram- en pofkraken.

> Daders hebben een bepaalde, voorspelbare reactie als zij vluchten. In de betreffende applicatie wordt daarom gebruik gemaakt van data van eerdere vluchtsituaties. Deze data zijn op systematische wijze opgenomen in een database. Vervolgens is (automatisch) naar patronen gezocht. Deze patronen zijn gebruikt om een algoritme te ontwikkelen waarmee de meest waarschijnlijke vluchtroutes kunnen worden berekend vanaf de locatie waar een delict heeft plaatsgevonden. Er is per delict een algoritme nodig. De uitkomsten van deze berekeningen worden door medewerkers gebruikt om het politieoptreden aan te sturen.

Er worden daarnaast systemen ontwikkeld en gebruikt die verdachte situaties in het straatbeeld detecteren. De data uit sensoren worden dan vergeleken met een profiel dat is ontwikkeld en een verdachte situatie representeert. De politie in Nederland heeft onder andere met deze werkwijze geëxperimenteerd in de proeftuin sensing in het kader van de aanpak van

[25] Landman & Groothuis 2022.

mobiel banditisme in Roermond.[26] Doel van deze proeftuin was het – buiten het winkelgebied – tegenhouden van potentiële daders van mobiel banditisme. Hiertoe is een profiel ontwikkeld, bestaande uit een aantal profielregels. Hierbij moet worden gedacht aan het merk en model van het voertuig, het land van herkomst van het voertuig, het aantal inzittenden en de route die het voertuig neemt. De data worden verzameld door verschillende sensoren en dan in het bijzonder ANPR-camera's. De data die op verschillende plekken worden verzameld, worden vergeleken met dit profiel en dit leidt tot een risicoscore. Een hoge risicoscore wordt als een 'hit' doorgegeven aan dienstdoende politieagenten, die bepalen of zij het betreffende voertuig stilhouden en eventueel nader controleren.

De – inmiddels beëindigde – proeftuin in Roermond is een voorbeeld van een bredere trend: het gebruik van systemen die verdachte burgers detecteren door hen op basis van algoritmische analyse in een risicogroep te plaatsen. De verwachting is dat er in de komende jaren meer van dit soort systemen in Nederland worden gebruikt.[27]

15.3.6. Veiligheidsanalyse

De toename van beschikbare data binnen de politie en de beschikbaarheid van digitale technologieën kunnen ook van grote waarde zijn voor analyse in het kader van intelligence.[28] Het gaat dan onder andere om het analyseren van veiligheidsproblemen ten behoeve van de sturing van politiewerk. Dit wordt ook wel veiligheidsanalyse genoemd.[29] Veiligheidsanalyses spelen een belangrijk rol in onder andere de aanpak van de georganiseerde criminaliteit. Door middel van veiligheidsanalyse wordt beoogd om meer inzicht te krijgen in de criminele wereld.

Binnen de Teams Criminele Inlichtingen van de politie is een analysemethode ontwikkeld waarmee de criminele wereld in kaart kan worden gebruikt. Deze methode heet Hyperion en bestaat uit een gestandaardiseerd model dat wordt gebruikt om gegevens van een classificatie te voorzien.[30] Aan gegevens kan onder andere een criminele markt, een fase in het criminele proces, een rol en een locatie worden toegevoegd. Ongestructureerde data – teksten die zijn opgenomen in criminele informatierapporten – worden op deze wijze gestructureerd. De data worden opgenomen in een relationele database en kunnen worden gebruikt om analyses te verrichten en de criminele wereld inzichtelijk te maken. Deze manier van werken ligt onder andere ten grondslag aan het Nationaal Inlichtingenbeeld Ondermijning.

Het gebruik van Hyperion heeft zich uitgebreid van de criminele inlichtingen naar de intelligenceorganisatie als geheel. Dit wil zeggen dat data uit verschillende bronnen – basispolitiezorg, opsporingsonderzoeken en criminele informatierapporten – worden geclassificeerd, gecombineerd en geanalyseerd. Er is en wordt technologie ontwikkeld om het classificeren van data te vereenvoudigen en de kwaliteit van de classificatie te verbeteren. De intelligencepositie die door het classificeren en combineren ontstaat, wordt gebruikt om veiligheidsbeelden te maken waarmee criminele netwerken en processen inzichtelijk worden gemaakt. Deze beelden kunnen worden gebruikt voor het prioriteren van veiligheidsproblemen, het ontwikkelen van interventiestrategieën voor de aanpak van veiligheidsproblemen en het starten van interventies, waaronder opsporingsonderzoek.

---

[26] Amnesty International 2020; Stevens et al. 2021.
[27] Stevens et al. 2021.
[28] Kirby & Keay 2021.
[29] Reijneveld 2017.
[30] Van der Plas & Brown 2017.

15.3.7. Predictive policing

Een van de meest meeslepende ideeën die voortvloeit uit het gebruik van artificiële intelligentie in het politiewerk is de mogelijkheid om criminaliteit te voorspellen en deze voorspellingen te gebruiken om te anticiperen op criminaliteit die gaat plaatsvinden.[31] Dit idee is in het afgelopen decennium in een groot aantal landen tot ontwikkeling gekomen onder de noemer van predictive policing.[32] Ook in Nederland wordt gebruik gemaakt van dit concept.

De eerste en meest toegepaste vorm van predictive policing is predictive mapping: het voorspellen van de plaatsen en momenten waarop criminaliteit gaat plaatsvinden. In Nederland maken alle basisteams gebruik van het Criminaliteit Anticipatie Systeem (CAS). Het CAS gebruikt uiteenlopende historische data – waaronder de geregistreerde criminaliteit, demografische data en sociaaleconomische gegevens – en berekent per gebied van 125 bij 125 meter hoe groot het risico op bepaalde delicten is in een bepaalde tijdsperiode. De kaarten die op basis hiervan ontstaan, worden door medewerkers van de intelligenceorganisatie gebruikt om inzetadviezen voor de basisteams te maken. Het doel hiervan is om politiecapaciteit in te zetten op de plaatsen en momenten die ertoe doen. Nederland is het eerste land ter wereld dat predictive mapping op nationale schaal heeft geïmplementeerd.

De tweede vorm van predictive policing is predictive identification: risicotaxatie op persoonsniveau. Hierbij gaat het om de vraag hoe groot de kans is dat een persoon (opnieuw) criminaliteit gaat plegen. Deze vorm van risicotaxatie is niet nieuw. Klinische, expertmatige inschattingen van het risico op recidive vinden al decennialang plaats. Sinds het jaren tachtig van de vorige eeuw zijn deze klinische beoordelingen in toenemende mate vervangen door risicotaxatie-instrumenten die gebruik maken van statistische methoden. Het gebruik van deze instrumenten heeft zich in de afgelopen decennia uitgebreid. Risicotaxatie vindt op dit moment plaats in allerlei fasen en bij allerlei doelgroepen, waaronder bij jongeren van 12-18 jaar die nog geen strafbare feiten hebben gepleegd. In Nederland wordt op dit moment vooral gebruik gemaakt van traditionele risicotaxatie-instrumenten. Deze instrumenten werken op basis van een model-gedreven algoritme. De internationale trend is dat de model-gedreven algoritmen steeds meer worden vervangen door data-gedreven algoritmen.[33] De verwachting is deze machine learning risicotaxatie-instrumenten accurater kunnen voorspellen, omdat er meer en complexere verbanden kunnen worden gelegd dan bij de traditionele risicotaxatie-instrumenten. Het is aannemelijk dat de politie in Nederland meegaat in deze ontwikkeling.

15.4.Gevolgen voor de politie

15.4.1. Model: data-gedreven politiewerk

De veranderende rol van digitale technologie in het politiewerk heeft geleid tot de introductie van een nieuw politiemodel of een nieuwe politiële strategie, die in internationaal verband big data policing of data-driven policing wordt genoemd.[34] In Nederland wordt veelal de term data-gedreven politiewerk gebruikt. De essentie van dit politiemodel is dat het politiewerk wordt gebaseerd op complexe analyses van grote hoeveelheden data uit verschillende bronnen.[35] Data worden hierdoor in toenemende mate leidend in het politiewerk. De politie in

[31] Ferguson 2017.
[32] Meijer & Wessels 2019.
[33] Berk 2021; Bland 2020; Hamilton 2021.
[34] Ferguson 2017; Kearns & Muir 2019; Marciniak 2021.
[35] Terpstra & Salet 2020.

Nederland heeft data-gedreven politiewerk geoperationaliseerd in een werkproces dat bestaat uit vier fasen: verzamelen, opslaan, analyseren en interveniëren.[36] Dit werkproces is ontstaan in het kader van de bestrijding van cybercriminaliteit en heeft zich in de afgelopen jaren uitgebreid naar steeds meer politieprocessen en inhoudelijke thema's.[37]

Data-gedreven politiewerk lijkt op intelligencegestuurd politiewerk waarbij beslissingen over de aanpak van veiligheidsproblemen en de uitvoering van de politietaak worden genomen op basis van geanalyseerde informatie en kennis.[38] Intelligence moet hierbij worden opgevat als sturingsinformatie. Data-gedreven politiewerk omvat echter meer dan intelligencesturing. Het proces van verzamelen, opslaan, analyseren en interveniëren wordt ook in toenemende mate toegepast in opsporingsonderzoeken waarin het niet gaat om sturingsinformatie, maar om bewijsmiddelen. Digitaal forensische zoekmachines en geavanceerde analysesoftware zijn hier voorbeelden van (zie paragraaf 15.3.2). Een tweede verschil tussen intelligencegestuurd politiewerk en data-gedreven politiewerk heeft betrekking op het gebruik van digitale, data-gedreven technologie in de breedte van het politiewerk. Dit betreft in het bijzonder artificiële intelligentie.[39] Door het gebruik van deze technologie wordt het vermogen van de politie tot het verzamelen en analyseren van data substantieel uitgebreid. Vaardigheden of talenten die voorheen werden beschouwd als menselijke vaardigheden – zoals het herkennen van verdachte situaties of het leggen van verbanden tussen informatie in opsporingsonderzoek – worden in toenemende mate ook en soms vooral uitgevoerd door digitale technologie. Deze ontwikkeling overstijgt de reikwijdte van intelligencegestuurd politiewerk. Dit rechtvaardigt de introductie van een nieuw politiemodel, te weten: data-gedreven politiewerk.

15.4.2. Organisatie: implementatie en adoptie

De ontwikkeling naar data-gedreven politiewerk bevindt zich in een beginstadium: het gaat vaker om pilots en proeftuinen dan organisatiebrede implementaties. Daarnaast moet worden opgemerkt dat het gebruik van opkomende, digitale technologieën hand in hand gaat met investeringen om de basis op het gebied van informatie- en communicatietechnologie op orde te maken. Bijvoorbeeld: de ontwikkeling naar een digitaal procesdossier in de opsporing (basis) vindt tegelijkertijd plaats met de ontwikkeling van spraaktechnologie om een opgenomen verhoor automatisch om te zetten in tekst voor een proces-verbaal (innovatie).

De weg van ontwikkeling, eerste experimenten naar organisatiebrede implementatie en uiteindelijk het gewenste gebruik van digitale technologie ligt vol met uitdagingen.[40] Ik richt me hier eerst op het ontwikkelen en implementeren van digitale technologie in het politiewerk. Longitudinaal onderzoek naar technologisch innoveren (van idee tot realisatie) binnen de politie in Nederland laat zien dat diverse factoren van invloed zijn op dit proces.[41] Een deel van deze factoren bevorderen de ontwikkeling en implementatie, waaronder het inspelen op de behoeften van gebruikers, het leren van experimenten in de praktijk en de samenwerking in het projectteam. Dit zijn vooral sociale factoren. Het overgrote deel van de factoren heeft een overwegend belemmerend effect op de ontwikkeling en implementatie van digitale technologieën. Het gaat dan onder andere om onduidelijke doelstellingen, gebrek aan (continuïteit in) capaciteit en kwaliteit in projectteams, onduidelijke aansturing, samenwerkingsproblemen tussen landelijke projecten en de operationele eenheden,

[36] Van de Sandt et al. 2022.
[37] Roest 2023.
[38] Kop & Klerks 2009.
[39] Joh 2018.
[40] Ariel 2020; Ernst, ter Veen, Lam & Kop 2019.
[41] Ernst, ter Veen, Lam & Kop 2019; Ter Veen & Kop 2021.

tussentijdse wijzigingen in landelijke prioriteiten, gebrek aan betrokkenheid van management, weinig flexibiliteit in de bedrijfsvoering en ontbreken van wetgeving (waar soms ook moet worden gewacht). Dit zijn vooral organisatorische factoren. De organisatorische belemmeringen in de politieorganisatie zijn van invloed op de looptijd van de ontwikkeling en implementatie van digitale technologieën in het politiewerk. Uit het eerdergenoemde longitudinale onderzoek komt een gemiddelde looptijd – vanaf het eerste idee tot en met implementatie in de politieorganisatie – van negen jaar naar voren.[42]

Degenen die nieuwe technologieën in het politiewerk (laten) implementeren, verwachten vaak dat het politiewerk effectiever en/of efficiënter wordt (zie ook paragraaf 15.5.1). Men verwacht bijvoorbeeld dat predictive mapping wordt gebruikt om gerichter te surveilleren, zodat criminaliteit kan worden voorkomen of dat veiligheidsanalyses worden gebruikt om tot een probleemgerichte aanpak in plaats van een incidentgerichte aanpak van criminaliteit te komen. Dit beoogde gebruik van (uitkomsten van) technologie wordt technologie-adoptie genoemd.[43] Een rode draad in het empirisch onderzoek naar technologie-adoptie is dat het gebruik van technologie niet altijd overeenkomt met wat was beoogd. Het gebruik van nieuwe technologie wordt geregeld ingepast in de al bestaande manier van werken in plaats van dat er een nieuwe manier van werken ontstaat.[44] Technologie-adoptie is weerbarstig.

Deze weerbarstigheid wordt in de eerste plaats veroorzaakt door de dominante manier waarop uitvoerende politiemensen en hun direct leidinggevenden naar het politiewerk kijken. Dit worden ook wel ‘culturele frames’ genoemd.[45] Deze manier van kijken is van invloed op hoe technologie door uitvoerende politiemensen wordt gebruikt.[46] Bijvoorbeeld: als politieagenten het reageren op incidenten als de essentie van het straatwerk zien, dan zullen zij nieuwe technologie op een manier gebruiken die past binnen deze taakopvatting. De bestaande manier van werken wordt dan eerder versterkt dan veranderd. Hierbij speelt mee dat er in het implementatieproces vaak meer nadruk ligt op het operationele gebruik van nieuwe technologie dan op het strategisch gebruik ervan.[47] Bijvoorbeeld: in trainingen krijgen politiemensen aangeleerd hoe ze bepaalde software moeten gebruiken, maar wordt niet meegenomen hoe dit gebruik moet bijdragen aan een andere manier van werken.

Een tweede reden voor de weerbarstigheid van technologie-adoptie heeft te maken met de wijze waarop nieuwe technologie wordt ontvangen door uitvoerende politiemensen. Zij kunnen nieuwe, digitale technologieën ervaren als een bedreiging.[48] Het gebruik van algoritmen in het politiewerk kan er bijvoorbeeld voor zorgen dat de discretionaire ruimte van politiemensen afneemt en hun ervaringskennis een minder grote rol speelt dan voorheen. Hierdoor kan er weerstand ontstaan tegen de introductie van nieuwe technologieën in het politiewerk. Het kan er ook toe leiden dat technologie niet wordt gebruik op de manier zoals was bedoeld door degenen die het hebben geïntroduceerd en geïmplementeerd.

Technologie is dus niet deterministisch.[49] Het dwingt geen verandering af in de manier waarop het politiewerk wordt uitgevoerd. Of die verandering wordt gerealiseerd, is

[42] Ter Veen & Kop 2021; zie ook De Pauw 2019.
[43] Lum, Koper & Willis 2017.
[44] Brayne 2021; Ferguson 2017; Mali, Bronkhorst-Giesen & den Hengst 2017; Manning 2008.
[45] Ratcliffe, Taylor & Fisher 2020.
[46] Koper & Lum 2019.
[47] Koper, Lum & Willis 2014.
[48] Brayne 2021; Ratcliffe, Taylor & Fisher 2020.
[49] Waardenburg, Sergeeva & Huysman 2020.

afhankelijk van handelingen van verschillende actoren. Het gaat bij technologie-adoptie dus (ook) veel meer om sociale processen dan om technologische processen.

15.4.3. Vakmanschap: digitale bekwaamheid

Voor de adoptie van digitale technologie in het politiewerk is het van belang dat politiemedewerkers digitaal bekwaam zijn. Dit wil in de eerste plaats zeggen dat medewerkers beschikken over een digitale mindset of digitaal bewustzijn. Deze mindset gaat om hoe je als politiemedewerker naar het gebruik van digitale technologie in het politiewerk kijkt.[50] Het uit zich in de bereidheid om regelmatig stil te staan bij de vraag hoe je aansluit bij de technologische ontwikkelingen die in de samenleving en organisatie gaande zijn.[51] Een politiemedewerker die digitaal bewust is, is bereid om te investeren in diens eigen kennis om zodoende de werking van opkomende technologieën op een basisniveau te begrijpen en hierin bij te blijven. Je moet snappen waar de huidige netwerk- en informatiesamenleving over gaat en bijvoorbeeld basiskennis hebben van een algoritme. Op dit moment beschikken vooral politiemedewerkers in (digitaal) specialistische functies over een digitale mindset. Er is in meer algemene zin sprake van een kennistekort.[52]

Een tweede onderdeel van digitale bekwaamheid bestaat uit datavaardigheden. Het (goed) werken met data moet door politiemedewerkers worden geïntegreerd in het eigen werk.[53] Dit betreft onder andere betrekking op de invoer, verwerking en interpretatie van data. Politiemedewerkers moeten zich in toenemende mate ontwikkelen tot ‘reflectieve dataprofessionals’ die begrijpen hoe het eigen werk tot data leidt en hoe data worden gebruikt in het kader van digitale technologie.[54] Bijvoorbeeld: de rechercheur die begrijpt hoe gelabelde data worden gebruikt bij veiligheidsanalyse (zie paragraaf 15.3.6). Op dit moment zijn datavaardigheden binnen de politie beperkt aanwezig. Dit komt onder andere tot uiting in de wijze waarmee wordt omgegaan met invoer in systemen: deze invoer is onvolledig. Zo wordt restinformatie in opsporingsonderzoeken – die van waarde is voor de intelligencepositie – beperkt vastgelegd en wanneer dit wel wordt gedaan, worden hiervoor niet de juiste coderingen gebruikt.[55]

Een derde onderdeel van digitale bekwaamheid gaat over het gebruik van geavanceerde (analyse)software. Dit wordt voor politiemedewerkers in alle werkterreinen een groter onderdeel van het werk. Zij dienen vaardig te zijn in het gebruik – en enig begrip te hebben van hoe applicaties werken.[56] Met betrekking tot het begrip van de werking gaat het onder andere om hoe uitkomsten tot stand komen en welke conclusies hier (niet) aan kunnen worden verbonden. Hierbij kan onder andere worden gedacht aan rechercheurs die gebruik maken van digitaal forensische zoekmachines. Politiemedewerkers moeten kunnen uitleggen hoe de uitkomsten van geavanceerde software hun eigen proces van beeld-, oordeels- en besluitvorming hebben beïnvloed.[57] Analysevaardigheden worden in het verlengde hiervan steeds belangrijker.[58] Op dit moment is het werken met analysesoftware geen gemeengoed

[50] Gebaseerd op Leonardi & Neeley 2022.
[51] Gebaseerd op Aslander, Broere & Meinema 2021.
[52] Zie bijvoorbeeld Jansen et al. 2020.
[53] Roest 2023.
[54] Waardenburg 2021.
[55] Hage 2021; zie ook Van Wijk, Scholten & Bremmers 2016.
[56] Waardenburg 2021.
[57] Ferguson 2017.
[58] Den Hengst 2017; Klerks & Vink-Teeven 2020; Marciniak 2021.

binnen de politieorganisatie.[59] Voor veel medewerkers geldt dat zij (nog) niet beschikken over de juiste vaardigheden.[60]

Het vierde onderdeel heeft betrekking op de juridische aspecten van data-gedreven politiewerk (zie ook paragraaf 15.5.2). Hoe meer politiemedewerkers werken met allerlei data, hoe belangrijker kennis van wet- en regelgeving wordt die het werken met data reguleert. Dit betreft in het bijzonder de Wet politiegegevens. Het gaat hierbij om algemene principes – zoals doelbinding, proportionaliteit en dataminimalisatie – en specifieke onderdelen en artikelen die op het eigen werk van toepassing zijn. Politiemedewerkers zullen een goed begrip moeten hebben van wanneer welke juridische kaders aan de orde zijn en wat zij op basis daarvan wel en niet mogen. Ook hiervoor geldt dat er nog een wereld te winnen is.

Bovenstaande niet-uitputtende uiteenzetting laat zien dat het toenemende gebruik van digitale technologie in het politiewerk gevolgen heeft voor het vakmanschap dat van alle politiemedewerkers wordt gevraagd. Net als in andere organisaties die investeren in digitale technologie, wordt de samenwerking tussen politiemens en 'politiemachine' een belangrijker thema.[61] Gezien het huidige gat tussen wat qua digitale bekwaamheid wordt gevraagd en binnen de politieorganisatie aanwezig is, zijn investeringen hierin van belang.

15.5.Gevolgen voor de samenleving

15.5.1. Effectiever politiewerk?

De verwachtingen van het gebruik van nieuwe technologieën in het politiewerk zijn vaak hoog.[62] Degenen die het introduceren, gaan er veelal vanuit dat het leidt tot substantiële verbeteringen in (onder andere) de effectiviteit van het politiewerk. Er zijn vooralsnog geen onderbouwde uitspraken te doen over de mate waarin de verwachtingen ook worden gerealiseerd.[63] Dit heeft verschillende redenen. Ik noem er twee. Het is in de eerste plaats nog (te) vroeg om de effectiviteitsvraag te stellen. Het gebruik van opkomende, digitale technologieën in het politiewerk bevindt zich – zoals eerder aangegeven – in een beginstadium. Daarnaast kost het – mede vanwege de weerbarstige adoptie van technologie – tijd om tot andere manieren van werken te komen die moeten leiden tot de beoogde effectiviteit. De tweede reden hangt samen met de eerste reden: het gegeven dat veel ontwikkelingen zich in een beginstadium bevinden, is een van de oorzaken dat evaluatieonderzoek naar het gebruik van digitale technologie in het politiewerk schaar is. Het (evaluatie)onderzoek dat (inter)nationaal is verricht, heeft vooral betrekking op predictive policing en heeft wisselende uitkomsten.[64]

Hoewel de effectiviteitsvraag op dit moment niet goed kan worden beantwoord, is het wel mogelijk en zinvol om aan te geven op welke wijze digitale technologie tot meer effectiviteit in het politiewerk kan leiden. Wat zijn de mogelijkheden en hoe worden die veroorzaakt?

De eerste mogelijkheid is het voorkomen van criminaliteit: ingrijpen voordat een incident plaatsvindt. Het gebruik van digitale technologie in het politiewerk kan bijdragen aan het

[59] Roest 2023.
[60] Den Hengst 2017.
[61] Daugherty & Wilson 2018, 2022.
[62] Terpstra & Salet 2020.
[63] Grace 2023; Khalfa & Hardyns 2023; Schuilenburg 2023.
[64] Meijer & Wessels 2019.

voorkomen van criminaliteit wanneer criminaliteit (juist) wordt voorspeld en op basis hiervan wordt geïntervenieerd. Interveniëren moet hierbij breed worden opgevat. Een voorbeeld is het waarschuwen van mensen die mogelijk worden geliquideerd (zie paragraaf 15.3.1), maar het kan ook gaan om aanwezigheid van de politie op bepaalde plaatsen en tijden waardoor criminelen hun voornemen tot het plegen van criminaliteit niet in de praktijk brengen.

De tweede mogelijkheid is het detecteren van criminaliteit: het vaststellen van een strafbaar feit op het moment dat het plaatsvindt, zodat de daders vrijwel direct kunnen worden aangehouden. De potentiële bijdrage van digitale technologie aan het (beter) detecteren van criminaliteit vloeit voort uit de eerder behandelde uitbreiding van het waarnemingsvermogen van de politie (zie paragraaf 15.4.1). Een voorbeeld hiervan is de ANPR-camera die eraan heeft bijgedragen dat de (destijds) verdachten van de aanslag op Peter R. de Vries konden worden aangehouden op de A4 bij Leidschendam. Kortom: door gebruik te maken van digitale technologie kan de heterdaadkracht van de politie worden vergroot.

De derde mogelijkheid is het ophelderen van criminaliteit: het reconstrueren van gepleegde strafbare feiten, zodat verdachten kunnen worden geïdentificeerd, aangehouden en vervolgd. De potentiële bijdrage van digitale technologie aan het (vaker) ophelderen van criminaliteit vloeit uit de uitbreiding van het waarnemingsvermogen en informatie-verwerkende vermogen van de politie. Hierdoor zijn er steeds meer digitale sporen die kunnen worden verzameld, doorzocht en geanalyseerd. De vele succesvolle opsporingsonderzoeken op basis van cryptocommunicatiedata zijn een voorbeeld van de potentie van het gebruik van digitale technologie bij het ophelderen van criminaliteit.

De vierde en laatste mogelijkheid is het tegenhouden van criminaliteit: het reduceren of in ieder geval beheersbaar houden van een fenomeen c.q. veiligheidsprobleem. De potentiële bijdrage van digitale technologie aan het (beter) tegenhouden van criminaliteit vloeit vooral voort uit de uitbreiding van het informatie-verwerkende vermogen van de politie. Door veiligheidsanalyse kan er in potentie meer of beter inzicht worden verkregen in criminele processen en de netwerken die zich hiermee bezighouden. Op basis hiervan kunnen interventies worden uitgevoerd die het criminele proces daadwerkelijk verstoren, bijvoorbeeld in het productieproces of het financiële proces.

Mijn inschatting is dat het gebruik van digitale technologie in het politiewerk vooral gaat leiden tot meer effectiviteit in termen van detectie en opheldering van criminaliteit. Voor meer effectiviteit in termen van het voorkomen en tegenhouden van criminaliteit is sociale innovatie van groot belang, omdat dit een andere manier van werken van de politie vraagt.

15.5.2. Meer (vergaande) privacy-inbreuken?

Het recht op privacy is vastgelegd in internationale mensenrechtenverdragen, zoals artikel 8 van het Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM). Op nationaal niveau is het recht op privacy vastgelegd in artikelen 10 tot en met 13 van de Grondwet. Het recht op informationele privacy of gegevensbescherming is hier (nauw) mee verbonden. De doelstelling van het recht op privacy is het individu te beschermen tegen willekeurige inmenging door onder andere de overheid in diens privéleven. Het recht op privacy is echter niet absoluut.[65] Er kunnen zwaarwegende belangen zijn die voor de overheid aanleiding zijn om inbreuken te maken op de persoonlijke levenssfeer van burgers, waaronder handhaving van de openbare orde en het voorkomen en opsporen van

[65] Schermer 2022.

strafbare feiten. Deze inbreuken moeten voldoen aan voorwaarden. Een inbreuk moet een legitiem doel dienen, noodzakelijk zijn in een democratische samenleving en bij wet zijn voorzien.

Het gebruik van digitale technologie in het politiewerk leidt – zoals eerder aangegeven – tot een versterking van het waarnemingsvermogen van de politie. Digitale vormen van waarnemen – met sensoren, maar ook online monitoring – zijn meer continu en grootschaliger dan traditionele vormen van waarneming.[66] Hierdoor worden er meer (diverse) gegevens over burgers vergaard. De omvang van surveillance neemt toe en dit kan vaker resulteren in inbreuken op het recht op privacy van burgers. Naast omvang neemt ook de diepgang van surveillance toe. Dit komt doordat gegevens – met gebruik van digitale technologie – in toenemende mate worden gecombineerd en in samenhang worden geanalyseerd. Zo ontstaan nieuwe inzichten die een gedetailleerder of beter inzicht geven in de hand en wandel van burgers. Dit kan resulteren in meer vergaande inbreuken op het recht op privacy.[67]

Bij zowel de toenemende omvang als groeiende diepgang van surveillance moet een onderscheid worden gemaakt tussen onverdachte burgers en verdachte burgers. Digitale technologie wordt immers niet alleen ingezet voor het opsporen van strafbare feiten, maar ook ten behoeve van het vroegtijdig signaleren van risico's en optreden op basis hiervan. Hierbij kan onder andere worden gedacht aan het – met behulp van algoritmen – taxeren van risicovolle en verdachte personen. Er worden grote groepen onverdachte burgers in beeld gebracht om vervolgens bepaalde burgers in een hoge risicocategorie te plaatsen. Deze risicoburgers kunnen te maken krijgen met intensievere bemoeienis van de overheid in het algemeen en de politie in het bijzonder, terwijl zij (nog) niet worden verdacht van een strafbaar feit. De politieactiviteiten vinden allemaal plaats op basis van de algemene taakstellende bevoegdheid van de politie, die is gebaseerd op artikel 3 Politiewet, en zijn dus niet bij specifieke wet voorzien. Dit levert spanning op met betrekking tot de rechtmatigheid van het optreden. Daarnaast moet worden opgemerkt dat de activiteiten plaatsvinden buiten het strafvorderlijk kader, want het gaat om onverdachte burgers. De activiteiten van de politie worden niet getoetst door bijvoorbeeld een rechter en een risicoburger heeft ook geen rechten zoals een verdachte. Dit alles maakt dat de toenemende omvang en diepgang van surveillance door de politie vooral bij onverdachte burgers een risico voor de mensenrechten vormt.

Het bovenstaande neemt niet weg dat er ook bij verdachte burgers aandachtspunten zijn. Deze aandachtspunten hebben in de eerste plaats te maken met de constatering dat in opsporingsonderzoek in toenemende mate onderzoek van bulkgegevens plaatsvindt. Dit betreft gegevens over meerdere personen, die voor een deel geen verdachte zijn van een strafbaar feit. Deze gegevens worden wel door de politie bewaard en komen in de politiesystemen terecht zonder dat hiervoor een legitieme reden bestaat.[68] Het onderzoek van bulkgegevens is in het (gemoderniseerde) Wetboek van Strafvordering ook niet expliciet genormeerd. In de praktijk worden in specifieke gevallen – zoals bij de cryptocommunicatiedata – kaders opgesteld en oplossingen gevonden, maar de rechtsbescherming van burgers is gebaat bij wetgeving die meegroeit met wat de politie in de praktijk doet. Een tweede aandachtspunt heeft niet zozeer te maken me de vergaring van gegevens, maar met de verdere verwerking ervan. Naarmate de politie meer de beschikking heeft over omvangrijke datasets waarin gegevens over meerdere (nog onbekende) personen zijn opgenomen, verschuift het zwaartepunt van de privacy-inbreuk van de vergaring van

[66] Ferguson 2022; Marx 2016; Purshouse & Roberts 2023.
[67] Purhouse & Roberts 2023.
[68] Fedorova et al. 2022.

gegevens naar de verdere verwerking van die gegevens. De vergaarde gegevens zeggen namelijk nog niet zoveel – onder andere doordat de identiteit van de betrokken personen nog onbekend is – maar krijgen betekenis wanneer deze nader worden geanalyseerd en worden gecombineerd met andere gegevens. Op dat moment neemt de inbreuk op het recht op privacy van de betrokken burgers (verder) toe. Het (gemoderniseerde) Wetboek van Strafvordering reguleert de verwerking van gegevens echter niet of nauwelijks. Deze regulering is onderdeel van een andere wet: de Wet politiegegevens (Wpg). De scheiding tussen beide heeft als risico dat de rechtsbescherming van de burger tussen wal en schip beland.[69] De Wet politiegegevens kent minder sterke waarborgen dan het Wetboek van Strafvordering, bijvoorbeeld voor wat betreft het toezicht op de gegevensverwerking.

15.5.3. Meer ongelijke behandeling?

Burgers hebben in een democratische rechtsstaat niet alleen recht op privacy, maar (onder andere) ook recht op een gelijke behandeling door de overheid. Het gebruik van digitale technologie in het politiewerk kan op gespannen voet staan met dit mensenrecht. Deze spanning doet zich vooral voor bij predictive policing. Dit komt omdat er bij deze toepassing plaatsen en personen als risico worden getaxeerd met mogelijk intensievere politiebemoeienis als gevolg. Dit hoeft geen probleem te zijn in het kader van gelijke behandeling, maar het punt is: voorspellende algoritmen werken niet perfect. Er worden fouten gemaakt. Er zijn valspositieven: iets wordt aangemerkt als een hoog risico, terwijl het in werkelijkheid een laag risico is. En er zijn valsnegatieven: iets wordt aangemerkt als een laag risico, terwijl het in werkelijkheid om een hoog risico gaat. Neem als voorbeeld een proactieve controle: wie handelt op basis van een valsnegatief kan iemand die criminaliteit pleegt of gaat plegen, laten passeren, terwijl wie handelt op basis van een valspositief een onschuldige burger controleert.

Ongelijke behandeling ontstaat vooral wanneer de valsnegatieven en valspositieven – en het optreden op basis hiervan – ongelijk zijn verdeeld over groepen burgers in de samenleving. Dit heeft immers als consequentie dat bepaalde groepen burgers meer negatieve effecten ondervinden van het gebruik van digitale technologie door de politie dan andere groepen burgers, bijvoorbeeld doordat zij intensiever worden gecontroleerd. In verschillende (internationale) publicaties over het gebruik van digitale technologie is geconcludeerd dat burgers met een migratieachtergrond onevenredig veel te maken (kunnen) krijgen met deze negatieve effecten.[70] Een voorbeeld van een dergelijke situatie in Nederland is de Top400 aanpak in de gemeente Amsterdam. Jongeren worden, ook zonder dat zij strafbare feiten hebben gepleegd, op basis van risicotaxatie aangemerkt als risicojongere.[71] Dit leidt tot een persoonsgebonden aanpak waarin hulpverlening en repressie samengaan. Hoewel er onvoldoende gegevens zijn om het goed te kunnen vaststellen, zijn er indicaties dat jongeren met een migratieachtergrond onevenredig worden benadeeld door deze werkwijze.[72]

Om de effecten van voorspellende algoritmen op (on)gelijke behandeling te begrijpen, is het van belang in te gaan op de accuraatheid van dergelijke algoritmen. Valspositieven en valsnegatieven ontstaan doordat algoritmen resulteren in vertekening (bias).[73] Er zijn verschillende lagen van vertekening. De basis-laag van vertekening ontstaat doordat er bij

[69] Schermer 2022.
[70] Amnesty International 2020; Brayne 2021; Egbert & Leese 2021; Ferguson 2017; Hamilton 2021; Jansen 2022; Shapiro 2020.
[71] In de eerste fase van de Top400 aanpak is gebruik gemaakt van het risicotaxatie-instrument ProKid van de politie (zie paragraaf 15.3.7).
[72] Jansen 2022.
[73] Eckhouse, Lum, Conti-Cook & Ciccolini 2019.

risicotaxatie kenmerken over de groep worden gebruikt voor het doen van uitspraken over het individu. Bijvoorbeeld: het geslacht wordt gebruikt als een van de factoren bij het maken van voorspellen waarbij het zijn van man tot een hogere risicoscore leidt. Een groepskenmerk is echter nooit determinerend voor individueel gedrag en dus is er altijd sprake van vertekening. Deze vertekening doet zich voor bij alle vormen van individuele risicotaxatie.

De tweede laag van vertekening heeft te maken met het gegeven dat de data die worden gebruikt niet de werkelijke criminaliteit representeren.[74] De werkelijke criminaliteit wordt immers niet gemeten. Er is een onbekend dark number. Burgers doen niet van alle criminaliteit melding of aangifte en de politie is selectief in de criminaliteit waar zij naar op zoek gaat. Omdat er geen indicator is voor de werkelijke criminaliteit, worden er bij algoritmen proxies gebruikt, zoals de geregistreerde criminaliteit. De meeste vertekening ontstaat wanneer in algoritmen data worden gebruikt die door de politie worden geproduceerd, omdat deze data allerlei keuzes reflecteren die in de politieorganisatie worden gemaakt: welke problemen hebben prioriteit, naar welke plaatsen ga ik toe, op welke personen ben ik gericht, wie controleer ik wel en niet, wie houd ik wel en niet aan. Data die door burgers worden geproduceerd – onder andere op basis van aangiften – bevatten ook vertekening, maar kunnen minder gemakkelijk leiden tot een selffulfilling prophecy: een politie die haar eigen gelijk bevestigt door zich te richten op bepaalde plaatsen en burgers en vervolgens vooral over hen data naar binnenbrengt. Kortom: digitale technologie die gebruik maakt van data die door de politie zijn geregistreerd (over individuen), leidt tot het grootste risico op ongelijke behandeling van burgers.

De derde laag van vertekening heeft betrekking op de modellering van algoritmen. Degenen die algoritmen ontwikkelen – waaronder datawetenschappers – maken hierbij allerlei keuzes. Bij model-gedreven algoritmen gaat het onder andere om de variabelen en het gewicht die deze variabelen krijgen. Bij data-gedreven c.q. zelflerende algoritmen gaat het onder andere om de trainingsdata en feedbackdata die worden gebruikt. Deze keuzes hebben consequenties voor hoe algoritmen werken en hoe de algoritmische besluitvorming plaatsvindt. Algoritmen zijn niet neutraal, want aan de keuzes van mensen liggen waarden en betekenissen ten grondslag.[75] Het ontwerp van algoritmen kan leiden tot ongelijke behandeling. Zo wijst Amnesty International erop dat het algoritme dat is gebruikt in de sensing proeftuin in Roermond – zie paragraaf 15.3.5 – leidt tot discriminerende uitkomsten, omdat het land van herkomst van het voertuig als kenmerk in het risicoprofiel is opgenomen. Dit kenmerk leidt bij drie landen – in combinatie met andere (scores op) kenmerken – tot een hogere risicoscore.

De bovenstaande lagen van vertekening maken dat (voorspellende) algoritmen niet perfect werken. Hierbij moet wel worden opgemerkt dat er ook voor het gebruik van digitale technologie inschattingen in het politiewerk werden gemaakt. Neem proactieve controles: politiemensen voorspellen ook de kans dat er met bepaalde burgers en/of voertuigen iets aan de hand is. En die voorspellingen zijn ook niet perfect. Het is dus van belang dat de accuraatheid van algoritmen niet worden beoordeeld op basis van het ideaal van perfectie, maar op basis van de mate waarin deze een verbetering opleveren ten opzichte van het bestaande.[76] Er is reden om aan te nemen dat algoritmen niet meer vertekening bevatten dan menselijke oordelen (eerder minder), maar algoritmen zijn wel in staat om die vertekening op veel meer mensen toe te passen. Neem de sensing proeftuin: alle voertuigen en (aantal) inzittenden worden gesurveilleerd en beoordeeld. Hierdoor kan het aantal valspositieven in

[74] Hamilton 2021.
[75] Adensamer & Klausner 2021; McDaniel & Pease 2021.
[76] Berk 2021.

absolute zin gemakkelijk toenemen. Wanneer dit leidt tot (repressief) optreden van de politie, neemt ook het aantal gevallen van ongelijke behandeling toe.

15.5.4. Verstoorde machtsbalans?

In de Grondwet zijn niet alleen mensenrechten opgenomen, maar ook regels voor de inrichting van de Nederlandse staat. Deze regels waarborgen onder andere de scheiding van de uitvoerende, wetgevende en rechtelijke macht; de trias politica. Deze scheiding is voor de rechtsstaat essentieel, omdat deze – bij adequaat functioneren in de praktijk – zorgt voor machtsbalans en het voorkomen van machtsmisbruik. Het gebruik van digitale technologie kan deze machtsbalans – checks & balances – verstoren of ondermijnen.[77]

Het verstoren van de machtsbalans wordt vooral veroorzaakt doordat de ontwikkeling en het gebruik van digitale technologie door de politie zich veelal afspeelt buiten het gezichtsveld van politiek, rechtelijke macht en samenleving. De politie is als uitvoerende macht dominant: zij heeft de data, de experts en ontwikkelt de digitale technologie of koopt die in. De keuzes die worden gemaakt, zijn niet of nauwelijks onderdeel van democratische controle. Politici en ook magistraten hebben weinig grip op de ontwikkelingen die plaatsvinden en kunnen hun controlerende functie moeizaam uitoefenen. Het ontbreekt aan voldoende tegenkracht.[78] Dit doet zich niet alleen voor in het politiedomein, maar ook in andere maatschappelijke sectoren. In de fraudebestrijding zijn misstanden met algoritmen aangepakt nadat bezorgde burgers en maatschappelijke organisaties (Systeem Risico Indicatie) dan wel volhardende politici en journalisten (Toeslagenaffaire) jarenlang hebben ‘gestreden’ voor de rechten van burgers. Dit roept de vraag op wie eigenlijk nog meekijkt met de uitvoerende macht en diens datahonger.

Het meekijken met en controleren van de politie bij ontwikkeling en gebruik van digitale technologie wordt bemoeilijkt door gebrekkige transparantie. Dit wil zeggen dat er door de politie weinig inzicht wordt gegeven in welke digitale technologie waarvoor wordt gebruikt en hoe deze werkt. Deze geheimhouding wordt door de minister van Justitie en Veiligheid geregeld gelegitimeerd door te verwijzen naar het belang van opsporing en handhaving. Bij ingekochte software kan er daarnaast sprake zijn van bedrijfsgeheim, wat maakt dat de politie als gebruiker ook niet precies weet hoe het werkt. Een andere oorzaak van gebrekkige transparantie is dat machine learning algoritmen veelal inherent ondoorzichtig zijn. Het algoritme dat zich (relatief) autonoom ontwikkelt, wordt op den duur zo complex dat het zich onttrekt aan het vermogen van mensen om het te begrijpen. Bij het Criminaliteit Anticipatie Systeem (zie paragraaf 15.3.7) konden de betrokken datawetenschappers de totstandkoming van uitkomsten niet (meer) uitleggen, omdat de gebruikte technieken voor patroonherkenning te complex waren.[79] De kracht van een zelflerend algoritme is ook diens zwakte: doordat de cognitieve vermogens van mensen ruimschoots worden overtroffen, kunnen mensen ook niet meer interpreteren en uitleggen hoe een zelflerend algoritme tot uitkomsten komt.[80] Er gaat wat in en komt wat uit, maar wat daartussen nu precies gebeurt, is onduidelijk.[81]

Kortom: het gebruik van digitale technologie door de politie gaat gepaard met het risico van een verstoorde machtsbalans binnen de rechtsstaat. Dit risico heeft de wetgevende macht in toenemende mate op het netvlies. In de komende jaren komt er meer wetgeving die het gebruik van digitale technologie door (onder andere) de politie gaat reguleren en het toezicht

[77] Passchier 2021.
[78] Buitenweg 2021.
[79] Waardenburg 2021.
[80] Hung & Yen 2021.
[81] Bland 2020; Wilson 2018.

aanscherpt. De verordening op het gebied van artificiële intelligentie van de Europese Commissie – die naar verwachting vanaf 2024 ingaat – is in dit verband een belangrijke stap.

15.6.Digitale technologie en politiewerk

15.6.1. Van de randen naar de kern

Dit hoofdstuk is een inleiding op de rol van digitale technologie in het politiewerk. Het gebruik van opkomende, digitale technologieën in het politiewerk bevindt zich in een beginstadium. Dit neemt niet weg dat deze ontwikkeling relatief snel gaat. Er wordt door de politie in Nederland veel geïnvesteerd in onderzoek en ontwikkeling en de randvoorwaarden die hiervoor nodig zijn. Er een onderzoekslab op het gebied van artificiële intelligentie, er zijn technische platformen op het gebied van big data en machine learning, er zijn vele teams – ook in de operatie – die geavanceerde software ontwikkelen, er worden steeds meer specialisten aangenomen die bijdragen aan de ontwikkeling naar data-gedreven politiewerk, zoals datawetenschappers en data-engineers en er zijn vele ontwikkelprojecten. De politie in Nederland kan in internationaal verband dan ook worden beschouwd als een voorloper op het gebied van de ontwikkeling en het gebruik van digitale technologie in het politiewerk.[82]

De rol van technologie in het politiewerk is hierdoor langzamerhand aan het veranderen. In de afgelopen decennia is de politie informatie- en communicatietechnologie (ICT) gaan gebruiken ter ondersteuning van het politiewerk, bijvoorbeeld in de vorm van registratiesystemen. De opkomst van digitale technologieën – in het bijzonder artificiële intelligentie – heeft als gevolg dat de secundaire functie van technologie verandert in een (op onderdelen) primaire functie. Processen van betekenisgeving van politiemensen worden steeds meer versterkt of overgenomen door digitale technologie. Sociale controle van burgers wordt deels uitgeoefend door camera's en (andere) sensoren, risico's worden ingeschat door algoritmen en bewijs wordt gevonden door analysesoftware. Het is pril, maar de trend is eenduidig: technologie beweegt zich van de randen naar de kern van het politiewerk.

15.6.2. Tussen effectiviteit en legitimiteit

De veranderende rol van digitale technologie in het politiewerk leidt tot zowel de potentie van effectiviteit als tot maatschappelijke risico's.[83] De politie is 'waakzaam en dienstbaar aan de waarden van de rechtsstaat', maar moet erop letten dat het gebruik van digitale technologie in het politiewerk niet leidt tot praktijken die afbreuk doen aan deze waarden en daarmee de legitimiteit van de politie ondermijnen. Daarom is voorzichtigheid geboden bij de verdere ontwikkeling van een meer data-gedreven manier van werken. Het kan soms beter zijn om te vertragen en meer te leren over de effecten van het gebruik van digitale technologie in het politiewerk dan om in de vlucht vooruit allerlei onbedoelde gevolgen tegen te komen.

Literatuurlijst

Adensamer, A. & L.D. Klausner, Part man, part machine, all cop. Automation in policing, *Frontiers in Artifical Intelligence*, 2021, 4, p. 1-10.

Amnesty International, *We sense trouble. Automated discrimination and mass surveillance in predictive policing in the Netherlands*, Amsterdam: Amnesty International 2020.

[82] Testerink, Nieuwenhuizen & Bex 2023.
[83] Zie ook Ferguson 2017.

Ariel, B., Technology in policing: advocate, in: D. Weisburd & A.A. Braga (Eds.), *Police innovation. Contrasting perspectives*, Cambridge: Cambridge University Press 2020, p. 485-515.

Aslander, M., A. Broere & M. Meinema, *Ons werk is stuk. Tips en inzichten voor onderhoud en reparatie*, Den Haag: Uitgeverij Publiek Denken BV 2022.

Baricco, A., *The game*, Amsterdam: De Bezige Bij 2018.

Beaulieu, A. & S. Leonelli, *Data and society. A critical introduction*, London: Sage Publications 2022.

Berk, R.A., Artificial intelligence, predictive policing, and risk assessment for law enforcement, *Annual Review of Criminology*, 2021, 4, p. 209-237.

Bex, F. & H. Prakken, De juridische voorspelindustrie: onzinnige hype of nuttige ontwikkeling? *Ars Aequi*, 2020, 3, p. 255-259.

Bland, M., Algorithms can predict domestic abuse, but should we let them? in: H. Jahankhani, B. Akhgar, P. Cochrane & M. Dastbaz (Eds.), *Policing in the era of AI and smart societies*, Cham: Springer 2020, p. 139-156.

Brayne, S., *Predict and surveil. Data, discretion, and the future of policing*, Oxford: Oxford University Press 2021.

Buitenweg, K., *Datamacht en tegenkracht. Hoe we de macht over onze gegevens kunnen terugkrijgen*, Amsterdam: De Bezige Bij 2021.

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

Daugherty, P.R. & H.J. Wilson, *Radically human. How technology is transforming business and shaping our future*, Boston: Harvard University Press 2022.

Eckhouse, L., K. Lum, C. Conti-Cook & J. Ciccolini, Layers of bias: a unified approach for understanding problems with risk assessment, *Criminal Justice*, 2019, 2, p. 185-209.

Egbert, S. & M. Leese, *Criminal futures. Predictive policing and everyday police work*, London/New York: Routledge 2021.

Ernst, S., H. ter Veen, J. Lam & N. Kop, *Leren van technologisch innoveren. 'De techniek is niet zo spannend'*, Politieacademie 2019.

Fedorova, M.I., R.M. te Molder, M.J. Dubelaar, S.M.A. Lestrade & T.F. Walree, *Strafvorderlijke gegevensverwerking. Een verkennende studie naar de relevante gezichtspunten bij de normering van het verwerken van persoonsgegevens voor strafvorderlijke doeleinden*, Radboud University Press 2022.

Ferguson, A.G., *The rise of big data policing. Surveillance, race, and the future of law enforcement*, New York University Press 2017.

Ferguson, A.G., Why digital policing is different, *Ohio State Law Journal*, 2022, p. 1-32.

Fry, H., *Algoritmes aan de macht. Hoe blijf je menselijk in een geautomatiseerde wereld?* Amsterdam: De Geus 2018.

Grace, J., Exploring algorithmic justice for policing data analytics in the United Kingdom, in: A. Roberts, J. Purshouse & J. Bosland (Eds.), *Privacy, technology and the criminal process*, London/New York: Routledge, 2023, p. 18-38.

Hage, J., *De rijkdom van restinformatie. Een onderzoek naar het gebruik van restinformatie bij de strafrechtelijke aanpak van synthetische drugs in de eenheid Zeeland-West-Brabant*, Apeldoorn: Politieacademie 2021.

Hamilton, M., Predictive policing through risk assessment, in: J.L.M. McDaniel & K.G. Pease (Eds.), *Predictive policing and artificial intelligence*, London/New York: Routledge, 2021, p. 58-78.

Hengst, M. den, Keerpunt intelligence. Naar politiewerk in een informatiemaatschappij, *Het Tijdschrift voor de Politie*, 2017, 6, p. 26-29.

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

Jansen, F., *Top400. A top-down crime prevention strategy in Amsterdam*, Public Interest Litigation Project 2022.

Jansen, J., T. van Valkengoed, S. Veenstra & W.P. Stol, *Level-Up! Kennis voor politiewerk in een digitale samenleving*, Leeuwarden/Apeldoorn: NHL Stenden Hogeschool/Politieacademie 2020.

Joh, E.E., Artificial intelligence and policing: first questions, *Seattle University Law Review*, 2018, 41, p. 1139-1144.

Kassab, H. & J. Rosen, General trends in drug and organized crime on a global scale, in: H. Kassab & J. Rosen (Eds.), Illicit markets, organized crime, and global security, London: Palgrave Macmillan, 2019, p. 87-109.

Kearns, I. & R. Muir, *Data driven policing and public value*, London: The Police Foundation, 2019.

Khalfa, R. & W. Hardyns, De evaluatie van big data policing. Krijtlijnen voor het opzetten van een geschikt experimenteel evaluatiemodel, in: T. Snaphaan, W. Hardyns, A. van Dijk, R. Spithoven & R. van Brakel (Eds.), *Big data policing*, Oud-Turnhout/'s-Hertogenbosch: Gompel & Svacina, 2023, p. 179-206.

Kirby, S. & S. Keay, *Improving intelligence analysis in policing*, London/New York: Routledge, 2021.

Klerks, P. & K. Vink-Teeven, De inzet van data-analysetechnologie ter bevordering van de informatiegestuurde opsporing, in: J. Janssens, W. Broer, M. Crispel & R. Salet (Eds.), *Informatiegestuurde politie*, Oud-Turnhout/'s-Hertogenbosch: Gompel & Svacina, 2020, p. 163-176.

Koolstra, S., B. de Veer & T. Veltman, *Dit is kunstmatige intelligentie. Een introductie in de technologie die ons leven steeds meer bepaalt*, 's-Hertogenbosch: Van Haren Publishing, 2021.

Kop, N. & P. Klerks, *Doctrine intelligencegestuurd politiewerk*, Apeldoorn: Politieacademie, 2008.

Koper, C.S. & C. Lum, Technology in policing: critic. The limits of police technology, in: D. Weisburd & A.A. Braga (Eds.), *Police innovation. Contrasting perspectives*, Cambridge: Cambridge University Press, 2019, p. 517-543.

Koper, C.S., C. Lum & J.J. Willis, Optimizing the use of technology in policing: results and implications from a multi-site study of the social, organizational, and behavioural aspects of implementing police technologies, *Policing*, 2014, 2, p. 212-221.

Kruisbergen, E.W., E.R. Leukfeldt, E.R. Kleemans & R.A. Roks, *Georganiseerde criminaliteit en ICT. Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit*. Den Haag: Wetenschappelijk Onderzoek- en Documentatiecentrum, 2018.

Landman, W. & S. Groothuis, *Politiewerk op het web. Een verkennend onderzoek naar online gegevensvergaring*, Den Haag: Sdu Uitgevers, 2022.

Lauwaert, L., *Wij, robots. Een filosofische blik op technologie en artificiële intelligentie*, Leuven/Amsterdam: Uitgeverij LannooCampus, 2021.

Leonardi, P.& T. Neeley, *The digital mindset. What it really takes to thrive in the age of data, algorithms and AI*. Boston: Harvard Business Review Press, 2022.

Lum, C., C.S. Koper & J. Willis, Understanding the limits of technology's impact on police effectiveness, *Police Quarterly*, 2017, 2, p. 135-136.

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

Manning, P.K., *The technology of policing. Crime mapping, information technology, and the rationality of crime control*, New York: New York University Press, 2018.

Marciniak, D., *Data-driven policing. How digital technologies transform the practice and governance of policing*, Essex: University of Essex, 2021.

Marx, G.T., *Windows into the soul. Surveillance and society in an age of high technology*, Chicago: The University of Chicago Press, 2016.

McDaniel, J.L.M. & K.G. Pease, Policing, AI and choice architecture, in: J.L.M. McDaniel & K.G. Pease (Eds), *Predictive policing and artificial intelligence*, London/New York: Routledge, 2021, p. 79-110.

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

Passchier, R., *Artificiële intelligentie en de rechtsstaat. Over verschuivende overheidsmacht, Big Tech en de noodzaak van constitutioneel onderhoud*, Den Haag: Boom juridisch, 2021.

Pauw, E. de, Technologie in beweging, in: E. Devroe, A. Schmidt, L. Gunther Moor & P. Ponsaers (Eds.), *De essentie van politiewerk*, Oud-Turnhout/'s-Hertogenbosch: Gompel & Svacina, 2019, p. 81-90.

Politie, *Inzetkader gezichtsherkenningstechnologie politie. Een eerste kader ter toetsing van operationele inzetten*, Den Haag: Politie, 2023.

Purhouse, J. & A. Roberts, Introduction: criminal justice, technology, and the future of privacy, in: A. Roberts, J. Purshouse & J. Bosland (Eds.), *Privacy, technology and the criminal process*, London/New York: Routledge, 2023, p. 1-17.

Ratcliffe, J.H., R.B. Taylor & R. Fisher, Conflicts and congruencies between predictive policing and the patrol officer's craft, *Policing and Society*, 2020, 6, p. 639-655.

Reijneveld, R., Analyse, in: M. den Hengst, T. ten Brink & J. ter Mors (Red.), *Informatiegestuurd politiewerk in de praktijk*, Deventer: Vakmedianet, 2017, p. 133-145.

Roest, D., Big data en politiewerk, een onoverbrugbare kloof? Hoe TROI de brug slaat van big data naar politiewerk, in: T. Snaphaan, W. Hardyns, A. van Dijk, R. Spithoven & R. van Brakel (Eds.), *Big data policing*, Oud-Turnhout/'s-Hertogenbosch: Gompel & Svacina, 2023, p. 91-106.

Sadin, E., *Het tijdperk van de ik-tiran. Het einde van de gemeenschappelijke wereld*, Amsterdam: Wereldbibliotheek, 2021.

Schermer, B.W., *De gespannen relatie tussen privacy en cybercrime*, Leiden: Universiteit Leiden, 2022.

Schuilenburg, M.B., Big data policing. Schets van de belangrijkste vraagstukken, partijen en nieuwste trends in de praktijk, in: T. Snaphaan, W. Hardyns, A. van Dijk, R. Spithoven & R. van Brakel (Eds.), *Big data policing*, Oud-Turnhout/'s-Hertogenbosch: Gompel & Svacina, 2023, p. 53-70.

Shapiro, A., Reform predictive policing, *Nature*, 2017, 541, p. 458-460.

Smit, S., A. de Vries, R. van der Kleij & H. van Vliet, *Van predictive naar prescriptive policing. Meer dan vakjes voorspellen*, Den Haag: TNO, 2016.

Stephenson, D., *Big data ontrafeld. Neem betere zakelijke beslissingen met big data, data science en AI*, Culemborg: Van Duuren Management, 2018.

Stevens, L., M. Hirsch Ballin, M. Galič, S.S. Buisman, B. Groothoff, Y. Hamelzky, C. Lucas, K. Rasul & S. Verijdt, Strafvorderlijke normering van preventief optreden op basis van datakoppeling. Een analyse aan de hand van de casus "Sensingproject Outlet Roermond", *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 2021, 4, p. 234-245.

Molder, R.M. te, Digitaal forensische zoekmachines, effectieve verdedigingsrechten en de modernisering van het Wetboek van Strafvordering: is aanpassing van het conceptwetsvoorstel gewenst? *Boom Strafblad*, 2022, 5, p. 178-186.

Veen, H. ter & N. Kop, *Innovatiekracht versterken. Een longitudinale processtudie naar technologisch innoveren bij de politie 2017-2020*. Apeldoorn: Politieacademie, 2021.

Terpstra, J. & R. Salet, Big data policing als sociale praktijk, in: J. Janssens, W. Broer, M. Crispel & R. Salet (Eds.), *Informatiegestuurde* politie, Oud-Turnhout/'s-Hertogenbosch: Gompel & Svacina, 2020, p. 25-38.

Testerink, B., E. Nieuwenhuizen & F. Bex, Wat doet het ertoe dat je een mens bent? Autonome AI-systemen voor de politie, in: T. Snaphaan, W. Hardyns, A. van Dijk, R. Spithoven & R. van Brakel (Eds.), *Big data policing* (p. 121-134). Oud-Turnhout/'s-Hertogenbosch: Gompel & Svacina, 2023, p. 121-134.

Tops, P., *Ondermijning en datawetenschap: waar gaat dat over?* Tilburg: Tilburg University, 2022.

Sandt, E. van de, M. den Hengst, P. de Bruine, R. Westerhof & S. van der Maden, Het datagedreven bestrijden. Nieuwe loot aan de stam in de bescherming van de rechtsstaat, in: A. van Dijk, P. de Baets, L. Gunther Moor, E. Devroe & S. Zouridis (Eds.), *Politie en rechtsstaat in de gedigitaliseerde samenleving* (p. 117-129), Oud-Turnhout/'s-Hertogenbosch: Gompel & Svacina, 2022, p. 117-129.

Plas, A. van der & C. Brown, Inwinning, in; M. den Hengst, T. ten Brink & J. ter Mors (Red.), *Informatiegestuurd politiewerk in de praktijk*, Deventer: Vakmedianet, 2017, p. 179-192.

Wijk, A. van, L. Scholten & B. Bremmers, *Onbenutte kansen. Een onderzoek naar het gebruik van restinformatie in de opsporing*, Amsterdam: Reed Business, 2016.

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

Waardenburg, L., M. Huysman & M. Agterberg, *S.L.I.M. managen van AI in de praktijk. Hoe organisaties slimme technologie implementeren*, Haarlem: Mediawerf, 2020.

Wilson, D., Algorithmic patrol: the futures of predictive policing, In: A. Završnik (Eds.), *Big data, crime and social control*, London/New York: Routledge, 2018, p. 108-127.

Wetenschappelijke Raad voor het Regeringsbeleid, *Opgave AI. De nieuwe systeemtechnologie*, Amsterdam: Amsterdam University Press, 2021.

Yang, A., *Jouw baan gaat verdwijnen en dit is de oplossing. Artificial intelligence, basisinkomen en de wereld zonder werk*, Voorschoten: Bot Uitgevers, 2020.