POLITIE & Wetenschap

Politiewerk aan de horizon

Technologie, criminaliteit en de toekomst van politiewerk

W. Landman

bureau landman
werken op grensvlakken

Politiewerk aan de horizon

Politiewerk aan de horizon

Technologie, criminaliteit en de toekomst van politiewerk

Wouter Landman

POLITIE & Wetenschap

Meer informatie over deze en andere uitgaven kunt u verkrijgen bij:

Sdu Klantenservice
telefoon: 070 - 378 98 80
website: www.sdu.nl/service

Vormgeving omslag: Imago Mediabuilders, Amersfoort
Afbeelding omslag: Shutterstock
ISBN: 9789012408967
NUR: 600

Inhoudsopgave

Voorwoord

Inmiddels ben ik al zo'n twintig jaar als onderzoeker en veranderaar actief binnen de politie. Ik vraag me weleens af wat maakt dat het leuk en boeiend blijft. Een van de redenen is – denk ik – dat vrijwel alle maatschappelijke ontwikkelingen op de een of andere manier invloed hebben op de politie en het politiewerk. De voortschrijdende digitalisering in de samenleving is naar mijn idee een van de ontwikkelingen die de politie nu en in de toekomst het sterkst beïnvloedt. Dit komt door de 'dubbele' beïnvloeding: digitalisering beïnvloedt zowel de aard van het veiligheidsvraagstuk als de wijze waarop het politiewerk wordt uitgevoerd. Toen ik in 2018 *Big data policing* van Andrew Ferguson uit de Verenigde Staten las, was ik direct overtuigd: ik wil een boek schrijven over digitale technologie en politiewerk.

Overtuiging is een goed begin voor het realiseren van een voornemen, maar zeker geen garantie. Ik ben daarom blij dat het ongeveer vijf jaar later gelukt is. Aan de realisatie van dit boek hebben verschillende personen een bijdrage geleverd. Annemieke Venderbosch en Adriaan Rottenberg hebben dit initiatief vanuit Politie & Wetenschap financieel gesteund en daarnaast waardevolle feedback gegeven op eerdere versies van het boek. Ik wil daarnaast een woord van dank aan de politie richten. Dit boek is vooral gebaseerd op allerlei open bronnen, maar dit neemt niet weg dat mijn ervaringen met onderzoek en andere opdrachten bij de politie enorm hebben geholpen bij het maken van dit boek. De politie heeft mij in de afgelopen twintig jaar de mogelijkheid geboden om – ik leen deze woorden van Jan Nap – steeds verder door te dringen in de 'geheimen' van het vak en de organisatie. Dat waardeer ik zeer. Het laatste woord van dank gaat naar mijn vriendin. Ik heb in de afgelopen jaren vele vroege ochtenden en weekenden besteed aan het schrijven van dit boek. Mireille, bedankt voor jouw steun en flexibiliteit. Dit boek is nu gelukkig klaar.

Dat brengt me bij het slot van dit voorwoord: het heeft me nog nooit zoveel moeite gekost om een punt te zetten. Het kostte tijd om me het thema eigen te maken en te ontdekken wat ik erover wilde zeggen. Daarnaast is het thema voortdurend in beweging, wat maakt dat de punt die je wilt zetten nog weleens opschuift. Hoe dan ook, ik heb veel van het maken van dit boek geleerd. Ik hoop dat dit leerproces ook voor jou als lezer van meerwaarde is.

Wouter Landman,
augustus 2023

Lijst van afkortingen

AAP	Advanced Analytics Platform
ACM	Aanpak Criminele Machtsstructuren
AGI	Artificial General Intelligence
AI	Artificiële Intelligentie
AMvB	Algemene Maatregel van Bestuur
ANPR	Automatic Number Plate Recognition
AP	Autoriteit Persoonsgegevens
API	Application Programming Interface
AR	Augmented Reality
AVG	Algemene verordening gegevensbescherming
BVH	Basisvoorziening Handhaving
BVI	Basisvoorziening Informatie
CAS	Criminaliteit Anticipatie Systeem
CAT	Crypto Analyse Team
CATCH	Centrale Automatische TeChnologie voor Herkenning van personen
CBS	Centraal Bureau voor de Statistiek
CCTV	Closed-Circuit Television
CJIB	Centraal Justitieel Incassobureau
CSAE	Collect Store Analyze Engage
CTIVD	Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten
CVT	Computer Vision Technology
DDoS	Distributed Denial of Service
DIGIT	Digital Intrusion Team
DLR	Dienst Landelijke Recherche
DRIO	Dienst Regionale Informatieorganisatie
DROC	Dienst Regionaal Operationeel Centrum
DSO	Dienst Speciale Operaties
DUO	Dienst Uitvoering Onderwijs
EBIT	Evidence Based Investigation Tool
EBP	Evidence-based policing
EDPB	European Data Protection Board
EHRM	Europese Hof voor de Rechten van de Mens
EU	Europese Unie
EVRM	Europees Verdrag voor de Rechten van de Mens
FBI	Federal Bureau of Investigation

FIRE	Forensic Image Recognition Engine
FIV	Forensic Identification Vehicle
FO	Forensische Opsporing
FRC	Flexibel Reactieconcept
FSV	Fraude Signalering Voorziening
GDPR	General Data Protection Regulation
GDT	Gunshot Detection Technology
GPS	Global Positioning System
GPT	Generative Pretrained Transformer
HAVANK	Het Automatisch Vingerafdrukkensysteem Nederlandse Kollektie
HMICFRS	His Majesty's Inspectorate of Constabulary and Fire & Rescue Services
ICAI	Innovation Center for Artificial Intelligence
ICS	Industriële Controle Systemen
ICT	Informatie- en Communicatietechnologie
IGP	Intelligence-gestuurde Politie
ILP	Intelligence-led Policing
IoT	Internet of Things
IV	Informatievoorziening
ISA	Intelligent Speed Assistant
JenV	Justitie en Veiligheid
JIT	Joint Investigation Team
KMar	Koninklijke Marechaussee
KvK	Kamer van Koophandel
LAPD	Los Angeles Police Department
Lhtbi+	Lesbische vrouwen, homoseksuele mannen, transgender, biseksuele en intersekse personen (en 'anderen' die niet vallen binnen wat als standaard wordt gezien)
LLM	Large Language Model
LMIO	Landelijk Meldpunt Internetoplichting
LOCO	Landelijk Operationeel Coördinatie Overleg
ML	Machine Learning
MPC	Multi Party Computation
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NFI	Nederlands Forensisch Instituut
NFT	Non-Fungible Token
NIBO	Nationaal Inlichtingenbeeld Ondermijning
NLP	Natural Language Processing
NYPD	New York Police Department
OC	Operationeel Centrum
OGG	Online Gegevens Garing
OM	Openbaar Ministerie
OPP	Operationeel Politie Platform
OSINT	Open Source Intelligence

OVC	Opname Vertrouwelijke Communicatie
PC	Personal Computer
PD	Plaats Delict
PDP	Politie Data Platform
PET	Privacy Enhancing Technology
PGA	Persoonsgerichte aanpak
PGP	Pretty Good Privacy
POP	Problem-oriented policing
POR	Politieonderwijsraad
PPS	Publiek private samenwerking
PVR	Programma Vernieuwend Registreren
Pw	Politiewet
Quin	QUestion & INvestigate
RiHG	Risicotaxatie-instrument Huiselijk Geweld
ROB	Raad voor het Openbaar Bestuur
RPA	Robotic Process Automation
RTIC	Real Time Intelligence Center
SDT	Samenwerkingsplatform Digitale Toezichthouders
SNA	Sociale netwerkanalyse
STOA	Panel for the future of science and technology
Syndru	Synthetische drugs
SyRI	Systeem Risico Identificatie
TCI	Team Criminele Inlichtingen
TGO	Team Grootschalig Onderzoek
THTC	Team High Tech Crime
TIM	The Incredible Machine
TK	Tweede Kamer
TLL	Threat To Life
TOR	The Onion Router
TROI	Team Rendement Operationele Informatie
VCAT	Voorziening Crypto Analyse Teams
VK	Verenigd Koninkrijk
VNG	Vereniging Nederlandse Gemeenten
VS	Verenigde Staten
WEET	Website Evaluatie Tool
WGS	Wet gegevensverwerking door samenwerkingsverbanden
Wjsg	Wet justitiële en strafvorderlijke gegevens
Wob	Wet openbaarbaarheid bestuur
Wpg	Wet politiegegevens
WRR	Wetenschappelijk Raad voor het Regeringsbeleid

1 Politiewerk en digitale technologie

Dit boek gaat over de invloed van digitale technologie op de politie en het politiewerk. In dit hoofdstuk wordt ingegaan op de reden, totstandkoming, beperkingen, doelgroep en opbouw van het boek.

Thema van en reden voor dit boek

Sinds het ontstaan van de politie hebben technologische ontwikkelingen in de samenleving invloed op het politiewerk.[1] Deze invloed verloopt in essentie langs twee lijnen. Technologie heeft in de eerste plaats invloed op de aard van de criminaliteit en onveiligheid in de samenleving. De ontwikkeling van de auto tijdens de tweede industriële revolutie heeft bijvoorbeeld tot nieuwe vormen van verkeersonveiligheid in de samenleving geleid.[2] Technologie heeft in de tweede plaats invloed op de wijze waarop het politiewerk wordt uitgevoerd. De introductie van de politieauto en van informatie- en communicatietechnologie (ICT) tijdens de derde industriële revolutie hebben het bijvoorbeeld mogelijk gemaakt om in grotere gebieden te patrouilleren en sneller informatie uit te wisselen.[3]

De voorgaande alinea maakt impliciet duidelijk dat technologie een breed begrip is. Wat onder 'technologie' wordt verstaan, is afhankelijk van verschillende factoren, waaronder plaats en tijd.[4] Als gevolg van de digitale revolutie heeft er een verschuiving plaatsgevonden van mechanische en analoge elektronische technologie naar digitale en computertechnologie.[5] In de huidige samenleving heeft technologie dan ook vooral de betekenis van digitale technologie: microprocessoren in steeds meer apparaten, internetinfrastructuren die deze apparaten verbinden, applicaties die op deze apparaten kunnen worden gebruikt, datastromen die door deze applicaties worden gegenereerd, gebruik van deze datastromen in weer nieuwe technologieën en ga zo maar door. Dit boek gaat over de invloed van digitale technologie op het politiewerk.[6] Het behandelt zowel de veranderingen in de aard van de criminaliteit en onveiligheid waarmee de politie te maken heeft als het technologiegebruik door de politie en de (eventueel)

1 Ariel 2019; Byrne & Marx 2011; Chan 2001; Hammer & Byrne 2017; Koper & Lum 2019; Shapiro 2020.
2 Zie bijvoorbeeld Meershoek 2007. Zie voor een meer internationaal perspectief: McGuire 2017.
3 Ernst et al. 2019; Koper & Lum 2019.
4 Lauwaert 2021.
5 Snaphaan et al. 2023.
6 In het vervolg van het boek wordt met 'technologie' digitale technologie bedoeld. Ook de term 'opkomende technologieën' wordt regelmatig gebruikt. Naarmate het boek vordert, zal de term 'datagedreven' vaker worden gehanteerd. Dit wordt nader toegelicht (zie hoofdstuk 22).

daaruit voortvloeiende veranderingen in de sturing en uitvoering van politiewerk. Beide kunnen samenhangen, maar dat hoeft niet. Technologie wordt namelijk gebruikt voor de aanpak van traditionele criminaliteit en voor de aanpak van nieuwe vormen van criminaliteit.[7]

Een boek over technologie en politiewerk kan op ieder moment in de tijd worden geschreven. De reden dat ik het nu heb geschreven, is mijn vermoeden dat er in het politiewerk wezenlijke veranderingen gaande en aanstaande zijn als gevolg van technologie. De voortschrijdende digitalisering heeft veel invloed op de aard van de criminaliteit en onveiligheid in de samenleving en dit stelt de politie voor (nieuwe) uitdagingen. Daarnaast experimenteren politieorganisaties wereldwijd met opkomende technologieën om hun taken (beter) uit te voeren in een steeds verder digitaliserende omgeving.[8] Dit geldt (zeker) ook voor de politie in Nederland.[9] Deze opkomende technologieën – en dan in het bijzonder artificiële intelligentie (AI) – dringen vermoedelijk steeds verder door in het politiewerk. Dit heeft vervolgens weer allerlei consequenties voor de politieorganisatie en het politievakmanschap. Al met al verwacht ik dat het politiewerk als gevolg van technologie in de komende tien tot vijftien jaar meer gaat veranderen dan het in de afgelopen twintig tot dertig jaar is veranderd.

Met dit boek wil ik mijn vermoeden verkennen. Dit doe ik door me te richten op het politiewerk dat vandaag in kleine praktijken zichtbaar is en (over)morgen waarschijnlijk tot vollere wasdom komt en steeds breder in het politiewerk ingebed raakt. Hierbij heb ik ook oog voor ontwikkelingen die elders gaande zijn, in het bijzonder in het Verenigd Koninkrijk (VK) en de Verenigde Staten (VS). Vanuit de werkelijkheid van vandaag trek ik lijnen door naar (over)morgen. Zo verschijnt het *politiewerk aan de horizon*. Inzicht in het politiewerk aan de horizon is belangrijk, omdat het gaat over hoe politiewerk in de samenleving vorm krijgt. Wat voor een politie willen we in onze samenleving hebben?[10] Hier moeten we – politiemensen, gezagsdragers, bestuurders, politici en wetenschappers – het gesprek over voeren. Ik hoop dat dit boek bijdraagt aan dit gesprek.

Aard en totstandkoming van dit boek

Dit is een boek en geen onderzoeksrapport. Het boek is een weerslag van mijn verkenning naar het politiewerk aan de horizon. Deze verkenning is begonnen uit persoonlijke interesse in het thema technologie, criminaliteit en politiewerk. Vanaf 2018 heb ik allerlei bronnen over dit thema verzameld en gelezen. Na verloop van tijd ontstond de wens om van de verkenning een boek te maken. Het boek heeft een beschouwend karakter. Anders gezegd: het is een geïnformeerde beschouwing[11] over technologie, cri-

7 Zie ook Hayward & Maas 2021.
8 Ter Veen & Kop 2021.
9 Zie bijvoorbeeld het overzicht van Ernst & Kop 2018.
10 Zie Nap 2014 die deze vraag vanuit de politie stelt: wat voor een politie willen we zijn?
11 Deze term leen ik van Boutellier 2021.

minaliteit en politiewerk. Hierna licht ik toe welke bronnen ik heb gebruikt om tot de beschouwing te komen.

In de afgelopen jaren heb ik een groot aantal wetenschappelijke publicaties uit binnen- en buitenland verzameld over technologie, criminaliteit en politiewerk.[12] Dit literatuuronderzoek is niet vormgegeven als een systematische review. Een systematische literatuurreview heeft door de bank genomen betrekking op een specifiek onderwerp, zoals *predictive policing*[13], terwijl voorliggend boek een groot aantal onderwerpen in relatie tot technologie, criminaliteit en politiewerk behandelt. Een systematische literatuurreview is voor een dergelijke opzet – min of meer – onuitvoerbaar. Dit neemt niet weg dat ik zo veel mogelijk relevante en gevarieerde publicaties over ieder onderwerp heb verzameld. In een deel van de gebruikte publicaties wordt verslag gedaan van empirisch onderzoek naar het gebruik van technologie in politiewerk, terwijl een groter deel een meer beschouwend karakter heeft.[14] Publicaties uit de VS en het VK zijn oververtegenwoordigd. De voornaamste oorzaak hiervoor is dat in deze landen al langere tijd en ook meer wordt gepubliceerd over dit thema dan in ons land.[15] De situaties tussen landen verschillen, maar veel van de inzichten die elders zijn opgedaan, zijn tot op zekere hoogte ook relevant voor ons land.

Naast wetenschappelijke publicaties over technologie, criminaliteit en politiewerk heb ik gebruikgemaakt van (populair)wetenschappelijke publicaties en managementboeken over opkomende technologieën in het algemeen en AI in het bijzonder. Deze publicaties heb ik gebruikt om het technologisch decor te schetsen waarop het politiewerk aan de horizon zich afspeelt. Ik heb deze publicaties daarnaast benut bij het verkennen van de gevolgen van technologiegebruik in het primaire proces voor de ontwikkeling van de organisatie en het vakmanschap van medewerkers. De politie kan immers leren van ervaringen van anderen.

De derde bron van de verkenning bestaat uit allerlei mediaberichten uit binnen- en buitenland. Ik heb vooral in ons land de mediaberichtgeving over technologie, criminaliteit en politiewerk actief gevolgd. Van verschijnselen als de metaverse en deepfakes tot discussies over gezichtsherkenningstechnologie en discriminatie door algoritmen. Met betrekking tot gevolgen voor de samenleving heb ik me breder georiënteerd dan het politiewerk en ook (een deel van) de ontwikkelingen in de fraudebestrijding meegenomen. Onder mediaberichten schaar ik voor het gemak ook de vacatures bij de politie die worden gepubliceerd op www.kombijdepolitie.nl. Deze vacatures geven enig inzicht in de ontwikkelingen die binnen de politieorganisatie plaatsvinden op het gebied van digitale technologie.[16]

12 Zie hiervoor de literatuurlijst.
13 Zie bijvoorbeeld Meijer & Wessels 2019.
14 In deze beschouwingen wordt in de regel wel gebruikgemaakt van empirisch onderzoek.
15 Zie McDaniel & Pease 2021a.
16 Zie ook Schuilenburg & Soudijn 2021.

De vierde en laatste bron is mijn eigen praktijk. Sinds in 2018 mijn interesse in technologie en politiewerk is aangewakkerd, heb ik talloze politiemensen gesproken over hun ervaringen en opvattingen. Dit heb ik gedaan in het kader van uiteenlopende (lopende) onderzoeken en advies- of begeleidingsopdrachten. De inzichten die ik hierbij heb opgedaan, heb ik op onderdelen – en waar mogelijk – verwerkt in dit boek. Hiermee hoop ik de praktijk ook weer te voeden.

Beperkingen van dit boek
De aard en opzet van dit boek gaan gepaard met een aantal beperkingen, die bij het lezen in het achterhoofd moeten worden gehouden.

Het thema technologie en politiewerk is een veelomvattend thema. Dit boek beoogt een overzicht te geven met betrekking tot dit thema. Het brengt onderwerpen en inzichten bij elkaar.[17] Er worden in dit boek veel onderwerpen behandeld, maar er mist ook het nodige. Het gaat bijvoorbeeld meer over technologie in de domeinen intelligence en opsporing dan in de domeinen noodhulp, handhaving en dienstverlening. Daarnaast is er over de onderwerpen die worden behandeld vaak meer te zeggen dan ik doe. Ik heb bij voortduring gezocht naar een goede balans tussen breedte en diepte. Ik hoop dat ik deze balans in voldoende mate heb gevonden, maar ik kan niet uitsluiten dat de breedte soms ten koste van de diepte is gegaan.[18] Dit wil zeggen dat het kan voorkomen dat ik onvoldoende recht doe aan alle details met betrekking tot een onderwerp en/of aan alle perspectieven die op een onderwerp mogelijk zijn. Ik heb er soms ook voor gekozen om aanvullende opmerkingen, nuanceringen en discussies in voetnoten te plaatsen.

De tweede beperking heeft betrekking op de voorbeelden van technologiegebruik door de politie die in dit boek worden behandeld. De beschrijving van deze voorbeelden is gebaseerd op open bronnen. Dit heeft er mogelijk toe geleid dat er bij sommige voorbeelden belangrijke elementen in de beschrijving ontbreken. Hierbij moet echter worden benadrukt dat de voorbeelden 'slechts' dienen als illustratie van een bepaalde ontwikkeling of type toepassing (*use case*). Bijvoorbeeld: de politie heeft samen met partners geëxperimenteerd met het gebruik van sensoren en risicoprofielen in de aanpak van mobiel banditisme in Roermond (zie hoofdstuk 17). Deze proeftuin is een illustratie van de bredere ontwikkeling die betrekking heeft op het geautomatiseerd detecteren van verdachte situaties of verdacht gedrag. De proeftuin in Roermond is inmiddels afgelopen, maar de bredere ontwikkeling van het geautomatiseerd detecteren van verdachte situaties of verdacht gedrag gaat door. Het gaat in dit boek om de bredere ontwikkelingen die gaande zijn. Bij ieder praktijkvoorbeeld zal ik zo duidelijk

17 Ik beschouw het niet zozeer als een beperking van dit boek, maar het is goed om te expliciteren dat het een theoriearm boek is.

18 Hierbij moet ook worden opgemerkt dat ik soms geen diepgang kon aanbrengen, omdat ik uitsluitend gebruik heb gemaakt van open bronnen. Bij sommige onderwerpen heb ik daardoor minder inzicht gekregen dan wanneer ik betrokkenen had geïnterviewd en/of inzicht had gekregen in interne politiepublicaties.

mogelijk aangeven wat de status is. In algemene zin kan worden geconstateerd dat het gebruik van opkomende technologieën door de politie op dit moment vaker de status heeft van een experiment dan van een breed geïmplementeerde praktijk. De vele experimenten die de politie uitvoert, zijn bedoeld om te leren over de mogelijkheden en onmogelijkheden van het technologiegebruik.[19] De wijze waarop een specifieke toepassing bij (eventuele) brede implementatie vorm krijgt, kan dus afwijken van de wijze waarop een experiment invulling heeft gekregen.

De derde beperking heeft te maken met de snelheid waarmee technologische ontwikkelingen zich voltrekken. In de aanloop naar publicatie van dit boek heb ik soms de opmerking gehoord dat de ontwikkelingen dusdanig snel gaan dat de inhoud van een boek als dit snel is achterhaald. Dit is inderdaad een beperking – of misschien wel het lot[20] – van een boek over het thema technologie, criminaliteit en politiewerk. Hierbij moet wel een aantal nuancerende opmerkingen worden gemaakt. De eerste opmerking is dat technologische ontwikkelingen binnen de politie zich in de regel helemaal niet zo snel voltrekken als de verhalen doen vermoeden. Uit longitudinaal onderzoek naar technologisch innoveren binnen de politie komt naar voren dat technologische innovaties een gemiddelde doorlooptijd – van eerste idee tot en met brede implementatie – van zo'n negen jaar hebben (zie ook hoofdstuk 23).[21] De tweede opmerking is dat de voorbeelden van de typen toepassingen sneller achterhaald zijn dan de bredere ontwikkelingen c.q. de typen toepassingen als zodanig. De relevantie van dit boek vloeit – zoals gezegd – meer voort uit deze bredere ontwikkelingen dan uit de specifieke praktijkvoorbeelden.

De vierde beperking van dit boek is dat er niet of nauwelijks aanbevelingen worden gegeven. De uitspraken die in dit boek worden gedaan, gaan vooral over de huidige situatie en over wat we in de toekomst kunnen verwachten. Op basis van inzicht in de huidige situatie en verwachte ontwikkelingen worden wel regelmatig aandachtspunten voor vooral de politie benoemd.

Tot slot: ik heb door het maken van dit boek veel geleerd over digitale technologie in het algemeen en de impact op de politie in het bijzonder. Ik hoop dat anderen door middel van dit boek kunnen profiteren van dit leerproces. Dit brengt me op het doel van dit boek: de lezer informeren over een thema dat nu en in de toekomst van groot belang is. Basiskennis over (de relatie tussen) digitale technologie, criminaliteit en politiewerk is naar mijn mening essentieel voor eenieder die binnen de politie werkt en voor een ieder die zich vanuit een externe positie met de politie bezighoudt.

19 In dit kader is het gebruik van gezichtsherkenningstechnologie door de politie een goed voorbeeld (zie hoofdstuk 14). De politie heeft in de afgelopen jaren geëxperimenteerd met 'realtime' gezichtsherkenning in een gecontroleerde omgeving – zonder daadwerkelijke operationele inzet – en dit heeft in 2023 geleid tot een inzetkader waarin de lessen zijn verwerkt.

20 Zie ook Snaphaan, Hardyns & Ponnet 2021.

21 Ter Veen & Kop 2021.

Doelgroep van dit boek
Dan de stap van doel naar doelgroep. Dit boek is in de eerste plaats bedoeld voor politiemensen die politiewerk uitvoeren, er leiding aan geven en erover adviseren. Zij hebben veelal[22] niet de tijd om op verkenning te gaan – zij hebben immers al een baan – dus ik hoop dat mijn verkenning hen helpt. Ik beschouw studenten in het veiligheidsdomein eveneens als een voorname doelgroep. Het gaat dan in het bijzonder om studenten die hoger politieonderwijs volgen. Opleiden is een toekomstgerichte activiteit en het is voor hen van meerwaarde om te begrijpen welke veranderingen in het politiewerk gaande en aanstaande zijn. Tot slot politiewetenschappers. Ik hoop dat dit boek hen overzicht biedt over diverse ontwikkelingen en vraagstukken op het gebied van technologie, criminaliteit en politiewerk. Ik verwacht dat dit overzicht voldoende aanknopingspunten biedt voor vervolgonderzoek. Deze verwachting baseer ik mede op een constatering die gedurende de verkenning onvermijdelijk was: het (empirisch) onderzoek naar de invloed van technologie op het politiewerk staat (in ons land) nog in de kinderschoenen.[23] Er is voldoende aanleiding om dit te veranderen.

Opbouw van dit boek
Het boek bestaat uit vijf delen. Ieder deel bestaat uit vier of meer (korte) hoofdstukken.

Deel I schetst het technologisch decor waarop het politiewerk zich afspeelt. Het gaat in op digitalisering, dataficatie, algoritmen en AI. Dit deel heeft een algemeen karakter – de politie komt er niet in voor – en beperkt zich tot enkele hoofdlijnen.

Deel II behandelt de invloed van technologie op het veiligheidsvraagstuk. De veelvoorkomende criminaliteit, de georganiseerde criminaliteit en een relatief nieuw vraagstuk dat 'maatschappelijk ongenoegen' wordt genoemd, komen in dit deel aan bod. Daarnaast wordt ingegaan op opkomende fenomenen, zoals deepfakes. De behandeling van de invloed van technologie op het veiligheidsvraagstuk is niet volledig. Ik heb me gericht op wat ik het meest relevant acht.

Deel III verplaatst de aandacht van het veiligheidsvraagstuk naar het politiewerk. Onder de noemer van 'technologiepraktijken' worden allerlei toepassingen van technologie in politiewerk behandeld. Zoals eerder aangegeven: de nadruk ligt hierbij vooral op intelligence en opsporing en minder op onder andere noodhulp en dienstverlening. De opbouw in het behandelen van de toepassingen is gebaseerd op een onderscheid in het tijdsperspectief:[24] van toepassingen die zich richten op het reconstrueren van het verleden (hoofdstuk 10 t/m 13), via toepassingen die betrekking hebben op het waarnemen van het heden (hoofdstuk 14 t/m 18) en dan naar toepassingen die beogen de

22 Er zijn binnen de politie vanzelfsprekend allerlei medewerkers van wie de baan primair gaat over het thema technologie, criminaliteit en politiewerk. Voor hen is dit boek vermoedelijk in mindere mate relevant.
23 Terpstra & Salet 2020; Schuilenburg & Soudijn 2021.
24 Dit is niet een heel strak onderscheid. Zo behandel ik online gegevensgaring bij het waarnemen van het heden, maar het wordt ook voor andere temporele oriëntaties gebruikt.

toekomst te voorspellen (hoofdstuk 19).[25] De toepassingen die worden behandeld, zijn soms – maar zeker niet altijd – een antwoord of reactie op het veranderende veiligheidsvraagstuk. Deel II en III zijn in dat opzicht twee 'losse' delen. Het ene deel gaat over de invloed van technologie op het veiligheidsvraagstuk en het andere deel over het gebruik van technologie in politiewerk.

Deel IV staat in het teken van de invloed van zowel het veranderende veiligheidsvraagstuk als het (toenemend) technologiegebruik op de politie.[26] Hierbij maak ik onderscheid tussen de politiefunctie, politievermogens, politiemodel, politieorganisatie, politiewerk en politievakmanschap. Dit is wellicht wat veel differentiatie, maar ik denk dat het nodig is om het verhaal te vertellen. De invloed op deze elementen onderbouw ik met (enig) empirische inzichten, maar het is voor een deel ook een invloed die ik verwacht of die wenselijk of noodzakelijk is. Dit verschil wordt in de tekst duidelijk.

Het vijfde en laatste deel gaat over de invloed van technologiegebruik door de politie op publieke waarden en dan in het bijzonder: effectiviteit, privacy, gelijke behandeling en het evenwicht der machten (checks-and-balances). Voor dit deel geldt dat het is gebaseerd op (enig) empirisch onderzoek en daarnaast op beschouwingen over de gevolgen van technologiegebruik op (specifieke) publieke waarden.

Ik sluit het boek af met een slothoofdstuk waarin ik de belangrijkste bevindingen op basis van de verkenning samenvat. In dit hoofdstuk keer ik terug naar de reden voor dit boek: in welke mate ondersteunen de opbrengsten van deze verkenning mijn vermoeden dat er in het politiewerk wezenlijke veranderingen gaande en aanstaande zijn als gevolg van technologie?

Tot slot twee opmerkingen. De eerste opmerking is dat de hoofdstukken separaat te lezen zijn, wat als gevolg heeft dat er soms sprake is van enige inhoudelijke overlap tussen hoofdstukken. De tweede opmerking is dat ik als schrijver, naarmate het boek vordert, meer aanwezig zal zijn in de tekst en meer normatieve uitspraken zal doen. Vooral deel 4 en 5 hebben een meer normatief karakter dan deel 1 tot en met 3.

25 Zie onder andere Terpstra & Salet 2020 en Wessels 2023 voor dit onderscheid.
26 De nadruk ligt meer op de invloed van technologiegebruik dan op de invloed van het veranderende veiligheidsvraagstuk.

Deel I Decor

2 Digitalisering

In rapporten waarin maatschappelijke ontwikkelingen worden beschreven, is digitalisering al enkele decennia een terugkerend begrip.[1] De digitalisering van de samenleving is een van de voornaamste aanleidingen voor dit boek. Daarom begint dit boek hiermee.

De basisinfrastructuur

Digitalisering is een uitvloeisel van de derde industriële revolutie die wordt gekenmerkt door de opkomst van informatie- en communicatietechnologie (ICT). De computer en het internet spelen hierin een centrale rol.[2] De eerste computers uit de jaren vijftig van de vorige eeuw waren 'mainframe computers' van enorme omvang. In 1971 vond er een doorbraak plaats: de introductie van de microprocessor van Intel. Deze microprocessor was slechts enkele millimeters groot, maar even krachtig als de reusachtige mainframes uit de jaren vijftig. De ontwikkeling van de microprocessor legde de basis voor de komst van de personal computer (pc) in de jaren tachtig van de vorige eeuw. In een tijdsbestek van vier jaar verschenen er drie van dergelijke computers: Commodore 64, IBM en Mac. Toen veranderde de wereld pas echt, aldus Alessandro Baricco in *The Game*.[3] Het ging volgens hem niet zozeer om de uitvinding van de computer, maar om het idee dat dit sindsdien een persoonlijk, individueel instrument is geworden. Met de komst van de pc deed een revolutionaire verandering in de fysieke en mentale houding van de mens zijn intrede: mens, knoppen en scherm.

> *'Vingers op de knoppen, ogen op het scherm. Opdrachten geven met de vingers, resultaten verifieerbaar met de ogen op het scherm. Voeg er nog een vleugje geluid aan toe, om het systeem functioneler te maken. Doet het je ergens aan denken? Het is tegenwoordig een van de fysieke en mentale houdingen waarin we het grootste deel van onze tijd doorbrengen.'*[4]

---

1 Ik geef in dit hoofdstuk geen afgebakende definitie van digitalisering en kies voor een brede invalshoek: de veranderingen die samenhangen met de komst van digitale technologieën en hun gebruik in de samenleving. Het is echter ook mogelijk om een onderscheid te maken tussen digitalisatie (van analoge naar digitale informatie), digitalisering (nieuwe processen en gebruiken rondom digitale technologie) en digitale transformatie (het geheel van veranderingen dat samenhangt met de komst en het gebruik van digitale technologieën). Zie de gids van Thamm, Gramlich & Borek (2020).

2 De inhoud van deze paragraaf is vooral gebaseerd op Barrico 2019 en Kool, Timmer & Royakkers 2017.

3 Barrico 2019.

4 Barrico 2019: 80.

In de jaren negentig volgde de opkomst van het internet. In de periode voorafgaand aan het internet waren er losstaande netwerken van computers. De doorbraak richting het internet vond plaats toen er een protocol (TCP/IP) werd ontwikkeld waarmee de netwerken onderling werden verbonden. En zo ontstond een wereldwijd netwerk: het internet. Volgens Baricco was aan het einde van de jaren negentig de basisinfrastructuur af.[5] In dit klassieke tijdperk van de digitale revolutie hebben we 1) de gegevens die de wereld bevatte tot een vloeibare toestand gereduceerd, 2) een eindeloos buizenstelsel aangelegd waar die vloeistof met duizelingwekkende snelheid doorheen kan stromen en waaruit hij in alle huizen van de mensen kon opborrelen, en 3) zeer geraffineerde kranen en wasbakken uitgevonden die kunnen dienen als terminals voor dat gigantische waterleidingnet. Hiermee werd de basis gelegd voor een samenleving van mens-toetsenbord-scherm. Kenmerkend voor dit wereldwijde netwerk is dat het primair buiten het politieke domein tot stand is gekomen.[6] De keuzes voor de inrichting van cyberspace zijn niet gemaakt via een democratisch politiek proces. Het eindeloze buizenstelsel van Baricco is primair privaat bezit.

Een digitale nevenwereld

Na de eeuwwisseling ontwikkelde het internet zich van een passief, informatie gevend medium – Web 1.0 – naar een interactief medium – Web 2.0 – waaraan gebruikers op allerlei manieren konden en kunnen bijdragen: via het geven van reacties, plaatsen van eigen content, beoordelen van de content van anderen et cetera. Sociale netwerksites, zoals Myspace, Hyves en Facebook, kwamen op en ook andere sociale media, zoals YouTube, deden hun intrede.

> *'Terwijl nog lang niet iedereen over internet beschikte, werd er alweer een nieuw systeem geïntroduceerd: het "Web 2.0". Deze naam betrof voor deze ene keer geen vage slogan, maar verwees daadwerkelijk naar nieuwe technieken die niet alleen toegang gaven tot een oneindige schat aan informatie, maar tevens verschillende mogelijkheden boden waarop de gebruiker zich ook actief kon inmengen op een website. Voor het eerst kon er "getagd" worden en werd het mogelijk om bijvoorbeeld op websites of onder aan een krantenartikel een commentaar te "posten". Voor iedereen werd het ineens doodeenvoudig om publiekelijk diens mening kenbaar te maken.'*[7]

In 2007 kondigde Steve Jobs van Apple de iPhone aan. Dit betekende een revolutie voor mobiele telefoons en de zogenaamde smartphone brak definitief door. De mobiele telefoon was vanaf dat moment niet meer alleen een telefoon, maar ook een computer die is verbonden met het internet en waarop gebruikers allerlei applicaties (apps) kunnen installeren en gebruiken. In de jaren daarna ontwikkelden de smartphone en

5 Barrico 2019.
6 Harari 2017.
7 Sadin 2021: 56.

andere mobiele apparaten (zoals tablets) zich in rap tempo door en hetzelfde gold voor draadloze internetverbindingen (3G en 4G).

Volgens Baricco waren sociale media en de smartphone de totems van de digitalisering tussen 2000 en 2010; een periode die hij definieert als kolonisatie. Hiermee bedoelt hij dat er met sociale media een nevenwereld is gecreëerd die is gekoppeld aan de gewone wereld. In die nevenwereld zijn we massaal tijd gaan doorbrengen. De smartphone heeft hierbij een cruciale rol gespeeld; deze werd een verlengstuk van de mens.[8] De houding mens-toetsenbord-scherm maakte zich door de komst van smartphone los van de pc en het werd mogelijk om 24 uur per dag, zeven dagen per week verbonden te zijn met de nevenwereld. Dit heeft ertoe geleid dat een steeds groter aandeel burgers steeds meer activiteiten online verricht.[9] We zijn steeds meer met onze ogen op schermen gericht.[10]

> *'Dat er in 2008 al 100 miljoen mensen op Facebook zaten, vonden we toen al ongelooflijk. Hyves en Second Life waren destijds booming. Nu zijn er alleen al in het online spel Fortnite 350 miljoen mensen te vinden. In 2020 telt Facebook 2,4 miljard gebruikers, YouTube 2 miljard, WhatsApp 1,6 miljard, TikTok 800 miljoen, Instagram 1 miljard en Reddit 382 miljoen gebruikers. Wereldwijd is men gemiddeld bijna zeven uur per dag op internet actief, waarvan tweeënhalf uur op sociale media.'*[11]

Barrico geeft aan dat merendeel van de burgers heeft geleerd de eigen persoonlijkheid te laten rondcirkelen over twee circuits waarvan we uiteindelijk hebben begrepen dat het de twee harten zijn van één enkel organisme: de realiteit. Hiermee geeft hij aan dat offline en online geen gescheiden werelden zijn, maar voortdurend in elkaar overlopen. De voortdurende wisselwerking tussen offline en online maakt dat er in de samenleving nieuwe fenomenen ontstaan en fenomenen van karakter veranderen. Een voorbeeld is straatcultuur.[12] Voorheen verwees straatcultuur naar normen, waarden, attitudes en uiterlijke verschijningsvormen die hun oorsprong vinden op de straten in gemarginaliseerde stedelijke omgevingen. De straatcultuur is door digitalisering echter losgezongen van de daadwerkelijke straten. Sociale media zijn een cruciale rol gaan vervullen in de ontwikkeling en verspreiding van straatcultuur: er is naast een fysieke straat nu ook een digitale straat.[13] Daardoor is de 'straat' in het fenomeen 'straatcultuur' tegenwoordig een hybride ruimte met wortels in de on- en offline werkelijkheid.[14] De straatidentiteit wordt in beide contexten ge(re)produceerd.

8 Ter vergelijking: de smartphone van tegenwoordig is ongeveer een miljoen keer krachtiger is dan de computers waarmee NASA in 1969 een man op de maan heeft gezet (Stolze, 2018).
9 Arets 2020. Zie ook https://www.cbs.nl/nl-nl/cijfers/detail/83429NED (voor het laatst geraadpleegd op 24 februari 2021).
10 Van Doorn, Duivesteijn & Pepping 2021.
11 Van Doorn, Duivesteijn & Pepping 2021: 17.
12 Van den Broek 2022; Roks, Leukfeldt & Densley 2020.
13 Lane 2019.
14 Van den Broek 2022; Roks, Leukfeldt & Densley 2020.

Het internet heeft een oneindig web van onderlinge contacten en verbindingen gecreëerd waarin mensen plaats- en tijdonafhankelijk werken, consumeren en produceren.[15] Doordat de objecten van de digitale revolutie massaal zijn geadopteerd door burgers is er in een periode van iets meer dan tien jaar – bezien vanaf de introductie van sociale media en smartphones – een volledig andere economische en (sociale) media-werkelijkheid ontstaan, met nieuwe conventies en daarmee gepaard gaande menselijke gedragingen.[16] In dat opzicht had de Spaanse socioloog Manuel Castells een vooruitziende blik toen hij aan het einde van de vorige eeuw schreef over de netwerksamenleving en het globale digitale kapitalisme dat zou gaan domineren.[17] Dit is in economisch opzicht onder andere zichtbaar in de lijst met bedrijven die de grootste beurswaarde vertegenwoordigen. De huidige lijst wordt aangevoerd door internationale, digitale bedrijven als Apple, Microsoft, Alphabet (Google), Facebook, Alibaba en Amazon, ook wel *Big Tech* genoemd.[18] Naar verwachting zal binnen afzienbare tijd grofweg de helft van het wereldwijde bruto binnenlands product bestaan uit digitale diensten.[19]

Ontwikkeling van de metaverse

Big Tech investeert op dit moment in de volgende fase van het internet: de metaverse.[20] Deze term kreeg bekendheid toen Facebook in 2021 diens naamverandering naar Meta (Platforms) aankondigde.[21] Maar wat is de metaverse? Ik gebruik de definitie van Matthew Ball:

> *'A massively scaled and interoperable network of realtime rendered 3D virtual worlds that can be experienced synchronously and persistently by an effectively unlimited number of users with and individual sense of presence, and with continuity of data, such as identity, history, entitlements, objects, communications, and payments.'*[22]

Deze definitie bevat veel kenmerken, die ik hier beperkt ga behandelen. Een van de meest essentiële of onderscheidende kenmerken van de metaverse is 3D. De metaverse behelst een fundamentele verandering of uitbreiding van het internet: het tweedimensionale, platte internet verandert met de metaverse naar een driedimensionale, ruimtelijke vorm.[23] In de metaverse zal de gebruiker zich in de digitale wereld (nog meer) verbonden voelen met het echte leven en het lichaam. Dit vindt plaats door toepassing van immersieve technologieën: technologieën die onze perceptie van de werkelijkheid

15 Lanting 2021.
16 Van Doorn, Duivesteijn & Pepping 2021.
17 Castells 1996.
18 De Wit 2021.
19 Lanting 2021.
20 McKinsey & Company 2022. Zie ook https://time.com/6197849/metaverse-future-matthew-ball/ en https://fd.nl/financiele-markten/1429332/financieel-bubbels-blazen-in-een-onbekende-virtuele-wereld (beide voor het laatst geraadpleegd op 20 juli 2022).
21 Zie https://about.facebook.com/meta/ (voor het laatst geraadpleegd op 27 december 2021).
22 Ball 2022: 28.
23 Winters 2021.

aanpassen door het aanbieden van alternatieve, sensorische informatie aan onze zintuigen.[24] Hierdoor kan de werkelijkheid worden aangepast, uitgebreid of in het geheel worden vervangen door een virtuele werkelijkheid. Gebruikers worden ondergedompeld in een alternatieve werkelijkheid waardoor een gevoel van fysieke aanwezigheid in die werkelijkheid ontstaat.[25] De gebruiker krijgt dus het gevoel dat de virtuele werkelijkheid echt is. Voorbeelden van dergelijke technologieën zijn augmented reality,[26] virtual reality[27] en spraaktechnologieën. De toepassing van deze technologieën moet leiden tot 'virtueel realisme': een virtuele wereld waarin alle kenmerken van de fysieke wereld aanwezig zijn. Als individu kun je in de metaverse 'echt' bestaan. Je hebt een avatar en je kunt je verplaatsen van locatie naar locatie om bijvoorbeeld grond te kopen, te gamen, concerten te bezoeken, te shoppen en te werken. De metaverse is hiermee (ook) een volgende stap in het creëren van een virtuele economie. In de virtuele economie van de metaverse is sprake van authentiek digitaal bezit door middel van een non-fungible token (NFT)[28] en kan worden betaald met cryptovaluta.[29]

De metaverse is op dit moment meer een ambitie en toekomstbeeld dan een realiteit.[30] Het bevindt zich nog in een prille fase.[31] Bepaalde bouwstenen – zoals blockchaintechnologie – zijn al behoorlijk ontwikkeld, maar tegelijkertijd zijn er nog de nodige technische beperkingen te overwinnen om tot de metaverse te komen die overeenkomt met de gegeven definitie. Zo zijn er veel krachtigere microprocessoren en videokaarten nodig om het virtueel realisme – het *realtime rendered* uit definitie – te bewerkstelligen.[32] Het duurt nog wel een jaar of tien voordat de metaverse 'net echt is', aldus Mark Zuckerberg van Meta.[33] Er zijn ook nog verschillende visies op de vorm die de metaverse zal krijgen. Wordt het een private vorm waarin internationale bedrijven bepalen hoe

24 Schermer & Van Ham 2021.
25 Roolvink, Kuijvenhoven & Huijstee 2022.
26 Bij augmented reality worden computergegenereerde beelden over de werkelijke wereld heen getoond, zodat je beide tegelijkertijd waarneemt. Dit betreft dus een uitbreiding of aanpassing van de perceptie van de fysieke wereld.
27 Virtual reality is een computergegeneerde, driedimensionale werkelijkheid die door de gebruiker wordt ervaren als een werkelijkheid waaraan die zelf deelneemt. De volledige werkelijkheid wordt dan vervangen door een virtuele werkelijkheid.
28 Een NFT is een cryptografisch ondertekend eigendomsbewijs dat wordt opgeslagen op een blokchain (op dit moment veelal Ethereum blockchain). Een blockchain is te zien als een online database die bestaat uit een keten van blokken. De blokken bestaan uit goedgekeurde transacties. Als er nieuwe transacties plaatsvinden, worden er nieuwe blokken aan de keten toegevoegd. De blokken moeten door een meerderheid van de deelnemers worden goedgekeurd. Er is geen derde partij, zoals een bank of notaris nodig. Cryptovaluta maken in de regel gebruik van blockchaintechnologie.
29 Madiega, Car & Niestadt 2022.
30 Zie ook https://jarnoduursma.nl/blog/wat-is-metaverse/ (voor het laatst geraadpleegd op 3 december 2021).
31 Er zijn vooralsnog verschillende werelden – zoals die van Roblox en The Sandbox – die los van elkaar staan. Niettemin: het gaming platform Roblox telt dagelijks 55 miljoen actieve gebruikers die meer doen dan gamen. Zo was er in oktober 2021 voor het eerst een meerdaags muziekfestival in Roblox. Zie ook https://time.com/6197849/metaverse-future-matthew-ball/ (voor het laatst geraadpleegd op 19 juli 2022).
32 https://fd.nl/financiele-markten/1429332/financieel-bubbels-blazen-in-een-onbekende-virtuele-wereld (voor het laatst geraadpleegd op 20 juli 2022).
33 https://www.nu.nl/tech/6207557/het-duurt-nog-even-voordat-de-metaverse-net-echt-is-denkt-ook-mark-zuckerberg.html (voor het laatst geraadpleegd op 20 juli 2022).

mensen kunnen leven in de metaverse of wordt het een gemeenschapsmodel waarin burgers gezamenlijk hun eigen wereld bouwen en besturen? Duidelijk is in ieder geval wel dat de internationale technologiebedrijven hun machtspositie willen behouden dan wel willen uitbreiden en (volop) inzetten op de realisatie van het virtuele universum van de toekomst. Het is daarmee ook zeer waarschijnlijk dat de metaverse er – in een bepaalde verschijningsvorm – gaat komen.[34]

De realisatie van de metaverse zal ertoe leiden dat het onderscheid tussen de 'gewone', fysieke wereld en digitale, 'nevenwereld' nog verder aan betekenis verliest. De nieuwe generatie virtualrealitybrillen – die naar verwachting al in 2023 op de markt komen – kunnen met camera's gezichtsuitdrukkingen herkennen en deze 'vertalen' naar de avatar.[35] Dit zal als gevolg hebben dat vrijwel alles wat we doen – nog meer dan bij het huidige internet – resulteert in data. Dit brengt ons bij het volgende hoofdstuk.

34 Roolvink, Kuijvenhoven & Huijstee 2022.

35 Zie https://www.nu.nl/tech/6219949/meta-introduceert-in-oktober-virtualrealitybril-die-gezichtsuitdrukkingen-herkent.html en https://www.nu.nl/tech/6220457/apple-virtualrealitybril-wordt-werkelijkheid-techgigant-vraagt-merknamen-aan.html (allebei voor het laatst geraadpleegd op 6 oktober 2022).

3 Dataficatie

Dataficatie is een begrip dat nauw samenhangt met digitalisering, maar niet hetzelfde is. Kennis van dataficatie is van belang voor het begrijpen van opkomende, digitale technologieën.

Steeds meer data

De digitalisering van het (samen)leven heeft onder andere als consequentie dat steeds meer menselijke handelingen worden omgezet in digitale data. Dit betreft zowel handelingen die voorheen ook plaatsvonden, maar niet digitaal werden vastgelegd (hardlopen) als nieuwe handelingen die zijn ontstaan door digitalisering (surfen op het internet).[1] Het resultaat is dat de meeste activiteiten van mensen die leven in een gedigitaliseerde samenleving data genereren.[2]

> *'Welke boodschappen we doen, waar we lopen en waar we rijden, wat we lezen, schrijven en met wie we bellen, ons energieverbruik, onze gezondheidsgegevens, schoolresultaten en werkprestaties: de groeiende hoeveelheid data die over ons wordt verzameld en opgeslagen is als een sneeuwbal die van een berg naar beneden rol en alsmaar groter wordt. En deze schijnbaar onstuitbare sneeuwbal heeft al jarenlang de wind in de rug.'*[3]

De groei van de data die (over ons) worden verzameld en opgeslagen, wordt onder andere veroorzaakt doordat steeds meer apparaten digitale data produceren.[4] Voorheen waren het vooral de computer en de smartphone die via het gebruik van allerlei applicaties digitale data produceerden, maar tegenwoordig worden aan de lopende band computerchips toegevoegd aan apparaten.[5] Hierbij kan worden gedacht aan allerlei apparaten voor het menselijk lichaam (zoals horloges), het huis (zoals deurbellen,

1 Snaphaan et al. 2023.
2 Beaulieu & Leonelli 2022.
3 Buitenweg 2021: 217.
4 Het is van belang op te merken dat digitale data uit getallen bestaan. Een digitale representatie van een foto bestaat uit een tabel met cijfers. Audio die digitaal is opgeslagen, wordt weergegeven als een aaneenschakeling van nummers. Kortom: als wij op de computer een afbeelding bekijken, dan zien we iets heel anders dan de computer 'ziet'. Zie hiervoor o.a. Maggiori 2023.
5 Stephenson 2018.

thermostaten, koelkasten), de werkomgeving (zoals sensoren in machines),[6] mobiliteit (zoals fietsen, auto's) en de leefomgeving (zoals straatverlichting, luchtmeters). Deze apparaten zijn in toenemende mate met elkaar en het internet verbonden én produceren digitale data.

Het enorme netwerk van onderling verbonden 'dingen', die gegevens verzamelen en deze uitwisselen, wordt het *Internet of Things* (IoT) genoemd.[7] In 2019 waren zo'n 10 miljard 'dingen' aan het internet gekoppeld.[8] In 2025 zijn dit naar verwachting zo'n 27 miljard apparaten en in 2030 zijn het er vermoedelijk 75 miljard of meer. Dit IoT zal naar verwachting een steeds grotere impact hebben op onze maatschappij en economie en zal rond 2025-2030 niet meer weg te denken zijn uit ons dagelijks leven. De overgang naar de vijfde generatie mobiele netwerken (5G) gaat bij de impact van IoT een belangrijke rol spelen, omdat 5G de snelheid en betrouwbaarheid van draadloze verbindingen enorm gaat verbeteren.[9] 5G gaat vooral een belangrijke bijdrage leveren aan het versturen en uitwisselen van data door IoT-apparaten en maakt zo tal van nieuwe toepassingen mogelijk.[10] De doorbraak van de zelfrijdende auto is *onder andere* hiervan afhankelijk, omdat zelfrijdende auto's continu met elkaar en met sensoren in de omgeving moeten communiceren. Dit vraagt veel van het mobiele netwerk.

Die in allerlei processen worden gebruikt

Het opslaan van de groeiende hoeveelheden data is in de afgelopen decennia steeds goedkoper geworden.[11] Er is hierdoor steeds meer data opgeslagen en beschikbaar. Het zijn schattingen, maar aangenomen wordt dat er in 2020 ongeveer 35 zettabyte aan data was opgeslagen en verwacht wordt dit in 2025 oploopt naar 175 zettabyte.[12] Eén zettabyte is een triljoen gigabyte. In de beeldspraak van NASA: één zettabyte is zoveel informatie als er zandkorrels op alle stranden ter wereld liggen.[13] Niet alleen de omvang van data neemt toe, ook de diversiteit in de data groeit. De verdere ontwikkeling van het internet zal ertoe leiden dat de diversiteit in data verder toeneemt, bijvoorbeeld voor wat betreft allerlei emotionele reacties die door een virtual reality headset kunnen worden gemeten.[14] De term *big data* wordt gebruikt om de enorme data-explosie te

6 Organisaties in de agrarische sector integreren bijvoorbeeld sensoren in hun productieproces, zodat gewassen kunnen worden gemonitord, irrigatiesystemen kunnen worden afgestemd op de toestand van de grond en (preventieve) reparaties voor machines kunnen worden voorspeld. Zie ook Hazenberg (2019).
7 Stephenson 2018.
8 Hazenberg 2019.
9 De Europese Unie (EU) beschouwt 'advanced connectivity' als de bouwsteen van de digitale transformatie en als aanjager van een duurzame toekomst. Zie hiervoor https://ec.europa.eu/digital-single-market/en/connectivity-european-gigabit-society (voor het laatst geraadpleegd op 30 december 2022).
10 Van Berkel et al. 2017.
11 Stephenson 2018.
12 https://magazines.informatiehuishouding.nl/rddimpact/2021/03/breng-de-informatiebeheerder-terug (voor het laatst geraadpleegd op 24 juli 2022).
13 https://mynasadata.larc.nasa.gov/basic-page/data-volume-units (voor het laatst geraadpleegd op 24 juli 2022).
14 Madiega, Car & Niestadt 2022.

duiden.[15] Bij big data gaat het over grote hoeveelheden (*volume*), gevarieerde (*variety*) data die met grote snelheid worden *verwerkt* (*velocity*).[16]

De verwerking van data is een belangrijk onderdeel van het proces van dataficatie. Dataficatie is namelijk het proces waarin menselijke handelingen worden omgezet in digitale data die vervolgens *in andere processen worden gebruikt*.[17] Het gaat dus niet alleen om de constatering dat steeds meer menselijke handelingen resulteren in data, maar ook om de wijze waarop deze data worden gebruikt om kennis te ontwikkelen en keuzes op te baseren.[18]

> *'The datafication of society is characterized by three main features. First, we see that the creation of data is becoming important and increasingly valued. Second, by using, combining and visualizing data in everyday life, data become even more central. And third, we take more and more decisions about current and future actions based on data.'*[19]

Bij het gebruik van data in andere processen – zoals besluitvorming – spelen algoritmen een belangrijke rol, omdat algoritmen data verwerken. Dit brengt ons bij het volgende hoofdstuk.

15 Beaulieu & Leonelli 2022; Lodder et al. 2014; Stephenson 2018.

16 Het begrip 'data' verwijst inmiddels dus niet meer alleen naar de 'gegevens', maar ook naar data als een concept (enkelvoud i.p.v. meervoud) dat in sociale, politieke, technologische en bedrijfsmatige zin betekenis heef. Zie hiervoor het boek *Data and society* van Beaulieu & Leonelli (2022).

17 Beaulieu & Leonelli 2022; Van Dijck, Poel & De Waal 2016.

18 Naast dataficatie is dataïsme een belangrijk begrip. Dataïsme is het geloof dat alles wat in de wereld bestaat in digitale data te vertalen is en dat daarmee de wereld de goede kant op te sturen is. Zie Rasch (2020) voor een kritische beschouwing van dit geloof.

19 Beaulieu & Leonelli 2022: 21.

4 Algoritmen

Volgens de Israëlische historicus Yuval Noah Harari is het concept 'algoritme' het allerbelangrijkste concept van onze huidige wereld. Als we iets van ons leven en onze toekomst willen begrijpen, moeten we goed begrijpen wat een algoritme is, aldus Harari in *Homo Deus*.[1] Hoewel er zeker kritiek mogelijk en ook nodig is op Harari zijn stelling dat 'algoritme' het allerbelangrijkste concept van onze wereld is[2], kan wel worden (vast)gesteld dat het concept 'algoritme' in de afgelopen twee decennia belangrijker is geworden. Dit hoofdstuk behandelt dit concept op hoofdlijnen.

Algoritme als begrip

Het woord 'algoritme' is eeuwenoud en gaat, naar het schijnt, terug tot een wiskundige in het Perzië van de 9de eeuw.[3] Een algoritme is een methodische reeks stappen die kan worden gebruikt om berekeningen te maken, problemen op te lossen en tot beslissingen te komen. Het is een serie logische instructies om een taak te volbrengen en iets voor elkaar te krijgen.[4] Hierbij kan worden gedacht aan een recept voor een taart of een handleiding voor het in elkaar zetten van een kast. Tegenwoordig heeft het begrip algoritme echter een meer specifieke betekenis. Het is een set aan instructies die in programmeertaal zijn vastgelegd, zodat een computer ze kan opvolgen.[5] Een *digitaal algoritme* zet inputdata via een geautomatiseerde reeks stappen om in outputdata.[6]

> **Een voorbeeld van een simpel algoritme**
> Neem als voorbeeld het voorspellen van woninginbraken. Een voorbeeld van een simpel algoritme voor het voorspellen van woninginbraken 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.[7]

1 Harari 2017.
2 Zie bijvoorbeeld het boek *Frictie* van Rasch (2020). De kritiek is vooral dat Harari alle organismen – 'van bacterie via baviaan en van baviaan helemaal tot aan de mens toe' – reduceert tot algoritmen.
3 Peeters & Schuilenburg 2021.
4 Berghdal 2020; Fry 2018; Stolze 2018.
5 Koolstra, De Veer & Veltman 2021.
6 Fry 2018; zie ook WRR 2016.
7 Smit et al. 2016: 17.

Bovenstaand (gesimplificeerd) voorbeeld geeft een indruk van hoe het concept van algoritme wordt gebruikt om van inputdata tot outputdata te komen. Er zijn verschillende typen algoritmen, bijvoorbeeld algoritmen die prioriteren, classificeren of associëren.[8] Alle algoritmen hebben met elkaar gemeen dat ze data verwerken.[9] Ze worden gevoed met data, hebben een doel en krijgen de taak berekeningen uit te voeren om hun doel te bereiken. Doordat algoritmen worden meegegeven aan microprocessoren met veel rekenkracht zijn ze in staat om grote hoeveelheden data te verwerken en hier inzichten en acties uit te genereren.[10] Een algoritme resulteert op deze wijze in een vorm van intelligentie, dit wil zeggen: de output van een algoritme is de oplossing van een – in wiskundige beweringen gedefinieerd – probleem.[11] Een algoritme stelt computers en andere apparaten in staat om zich intelligent te gedragen.[12] Algoritmische analyse is cruciaal in vrijwel alle opkomende technologieën, zoals als IoT, robotica, big data en AI. Algoritmen maken het mogelijk om door sensoren geregistreerde data te analyseren op een zodanige manier dat de data bruikbaar worden in een applicatie of voor de acties van een robot. Algoritmen zoeken de spreekwoordelijke speld in een hooiberg bij big data. En algoritmen zijn de bouwsteen van AI.

Expertsystemen en artificiële intelligentie

Er zijn twee hoofdverschijningsvormen van algoritmen.[13] De eerste verschijningsvorm is een op regels gebaseerd algoritme, ook wel een *modelgedreven* algoritme genoemd. De instructies worden in dit geval opgesteld door de mens en zijn veelal gebaseerd op een vorm van theorie. Bijvoorbeeld: als je de kans wil voorspellen dat mensen die zijn veroordeeld voor criminaliteit opnieuw een delict gaan plegen (recidive), dan kun je aannames doen over de factoren die hierop van invloed zijn en deze factoren een bepaalde zwaarte geven. Zo bouw je een theoretisch model in computercode. Als je vervolgens gegevens over iemand die is veroordeeld 'aan' het softwareprogramma geeft, dan berekent het algoritme de kans op recidive. Een wiskundige formule zorgt er dus voor dat inputdata leiden tot een nieuw inzicht. Het programma of systeem dat de berekening uitvoert, wordt een expertsysteem genoemd.[14] De reden hiervoor is dat de instructie of formule mensenwerk is. Expertsystemen zijn vanaf de jaren zeventig van de vorige eeuw opgekomen en representeren de eerste vorm van AI die in de praktijk is gebracht. Tegenwoordig wordt deze AI ook wel *Good Old Fashioned Artificial Intelligence* genoemd. Dit doet dus vermoeden dat er iets nieuws is gekomen.

8 Zie Stolze (2018) en Fry (2018) voor een overzicht van typen algoritmen. Hierbij moet worden opgemerkt dat er weinig consensus bestaat over hoe typen algoritmen het best kunnen worden ingedeeld. Zie ook hoofdstuk 5.
9 Zie o.a. Fry 2018 en Stolze 2018.
10 Vetzo & Gerards 2019.
11 Stolze 2018.
12 Hierbij moet worden beseft dat dit een specifieke vorm van intelligentie is die niet te vergelijken is met de meer algemene en veel bredere menselijke intelligentie (zie ook hoofdstuk 5).
13 Fry 2018.
14 Lauwaert 2021.

Het vastleggen en schrijven van regels in een expertsysteem kost veel tijd en een expertsysteem is niet adaptief: op het moment dat het in een situatie terechtkomt waarvoor geen regels zijn geschreven, dan doet het niets.[15] Onder andere vanwege deze beperkingen is er een nieuw type algoritme opgekomen: een *machine learning* algoritme, ook wel slim algoritme genoemd. Dit type algoritme werkt anders dan een expertsysteem: het is niet modelgedreven, maar *datagedreven*. Dit wil zeggen dat je een doel formuleert[16], data beschikbaar stelt en feedback geeft op de uitkomsten. Op basis hiervan zoekt de software de beste manier tot doelrealisatie uit. Terug naar het voorbeeld van recidive. Een van de mogelijkheden is om de computer een grote hoeveelheid historische gevallen te geven van veroordeelde personen die wel én geen recidive hebben gepleegd.[17] 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 worden een of meerdere modellen[18] ontwikkeld waarmee de kans op recidive kan worden berekend. Op basis van aanvullende datasets wordt het beste model geselecteerd en vervolgens verder getest.[19] Het algoritme dat nu is ontstaan,[20] is in de regel veel complexer dan een modelgedreven algoritme, omdat er tal van patronen worden gevonden die worden gebruikt voor het omzetten van de inputdata in de outputdata. Een machine learning model bevat al snel honderden of duizenden rekenstapjes.[21] Ook wanneer het algoritme in de praktijk wordt toegepast, wordt er idealiter voortdurend feedbackdata uit de omgeving – data over daadwerkelijk recidive van de betreffende personen – gebruikt om het algoritme te verbeteren. Dit leerproces heeft onder andere als gevolg dat regels dynamisch zijn: ze worden automatisch gewijzigd op basis van feedback uit de omgeving. Anders gezegd: een machine learning algoritme is adaptief.

Met machine learning is een manier gevonden om computers van data te laten leren.[22] De machine leert activiteiten zonder dat deze hier expliciet voor is geprogrammeerd.[23] Een machine learning algoritme is dan ook geïnspireerd op hoe levende levens denken.[24] Hiermee zijn we aanbeland bij het onderwerp van het laatste hoofdstuk van dit eerste deel: artificiële intelligentie.

15 Lauwaert 2021; Maggiori 2023; Mannens 2021; Pearl & Mackenzie 2019.
16 Dit klinkt iets gemakkelijker dan het is. Er wordt – veelal door een datawetenschapper – een template gemaakt waarbij de waarden worden ingevuld door de 'machine' te laten leren van data. Dit leidt tot het model c.q. algoritme. Zie o.a. Maggiori 2023.
17 Zie ook Bex & Prakken 2020.
18 Van meerdere modellen is bijvoorbeeld sprake bij een random forest algoritme.
19 In de testdata worden alleen de kenmerken – en niet de uitkomsten – meegegeven. Zo kan de betrouwbaarheid van het algoritme worden geëvalueerd.
20 Hierbij moet worden opgemerkt dat dit algoritme weliswaar is ontstaan op basis van data, maar er wel allerlei keuzes door mensen zijn gemaakt (zie ook hoofdstuk 24 over discretionaire ruimte). Bijvoorbeeld: bij het selecteren van de trainingsdata worden impliciet aannames gedaan met betrekking tot welke kenmerken mogelijk relevant zijn.
21 Koolstra, De Veer & Veltman 2021.
22 Fry 2018.
23 Berghdal 2020.
24 Het is nadrukkelijker 'geïnspireerd op' en niet 'gebaseerd op'. Anders gezegd: machine learning werkt anders dan (wat we weten over) hoe menselijke intelligentie werkt. Zie o.a. Maggiori 2023.

5 Artificiële intelligentie

We komen vrijwel allemaal dagelijks bewust of onbewust in aanraking met AI.[1] Je komt praktische toepassingen van AI tegen in het huis, de auto, op het werk, in het ziekenhuis en bovenal in allerlei applicaties op de smartphone. Er is volgens experts geen technologie die zoveel impact op onze samenleving heeft en gaat hebben als AI.[2] Volgens de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) is de impact van AI in deze eeuw te vergelijken met de impact van elektriciteit in de negentiende eeuw en de verbrandingsmotor in de twintigste eeuw.[3] AI is een *systeemtechnologie*: technologie die alomtegenwoordig is,[4] continue verbetering kent en complementaire innovatie mogelijk maakt. Dit hoofdstuk behandelt enkele kenmerken en aspecten van AI. Ik ga eerst in op de opkomst en definitie van AI en vervolgens op verschijningsvormen.

Korte historie en definitie van artificiële intelligentie

AI is niet nieuw.[5] In de zomer van 1956 werd de term 'artificiële intelligentie' voor het eerst uitgesproken.[6] In deze periode zijn de theoretische grondslagen voor AI gelegd, maar kon AI praktisch niet worden gerealiseerd.[7] Na de introductie van de (mainframe) computers vonden in de jaren zestig van de vorige eeuw de eerste investeringen in de daadwerkelijke ontwikkeling van AI plaats. Vooral door de Amerikaanse overheid. Na initieel enthousiasme over de mogelijkheden werd in het begin van de jaren zeventig duidelijk dat AI diens beloften niet kon inlossen. Zo konden er geen eenvoudige, automatische vertaalprogramma's worden gerealiseerd. De investeringen werden teruggeschroefd en de eerste 'AI-winter' was een feit. Vanaf de jaren tachtig ontstond er nieuw enthousiasme als gevolg van de opkomst van expertsystemen met geschreven regels voor het uitvoeren van taken c.q. oplossen van problemen (zie hoofdstuk 4). In deze periode investeerde ook delen van de private sector in de ontwikkeling van AI. De overwinning van IBM's schaakcomputer *Deep Blue* op Garry Kasparov in 1997 was een symbolische mijlpaal in de ontwikkeling van AI.[8] Maar ook nu volgde er een AI-win-

1 Boden 2018; Campbell 2022; Koolstra, De Veer & Veltman 2021; Peeters & Schuilenburg 2021.
2 Koolstra, De Veer & Veltman 2021; WRR 2021a.
3 WRR 2021a; zie ook Agrawal, Gans & Goldfarb 2022.
4 Dit wil onder andere zeggen dat het een technologie betreft die in vrijwel alle sectoren wordt gebruikt, in het Angelsaksisch ook wel *general purpose technology* genoemd (zie Agrawal, Gans & Goldfarb 2022).
5 Ik baseer de beschrijving van de historie vooral op Maggiori 2023 en Mannens 2021.
6 Mannens 2021.
7 Boden 2018; Stolze 2018; Hazenberg 2019; Maggiori 2023; WRR 2021a.
8 Fry 2018. Deep Blue had vooral het karakter van een expertsysteem met veel geprogrammeerde regels (zie hoofdstuk 4 voor de term 'expertsysteem').

ter. Het enthousiasme nam af. Expertsystemen hadden en hebben veel beperkingen, waaronder het beperkte aanpassingsvermogen (zie hoofdstuk 4).
De tweede AI-winter duurde tot omstreeks 2010. De overwinning van IBM's Watson op de twee beste menselijke Jeopardy spelers – Brad Rutter en Ken Jennings – in 2011 kan worden gezien als een belangrijk keerpunt: het begin van een nieuwe, derde opleving van AI. Deze opleving is nu gaande en verschilt wezenlijk van de tweede voorgaande oplevingen: de stap van de wetenschappelijke wereld naar de samenleving is definitief gemaakt.[9] De brede adoptie van AI in de samenleving die nu gaande is, is nieuw in de historie van AI. Deze doorbraak van AI is mogelijk gemaakt door verschillende factoren. De drie hoofdfactoren zijn in de voorgaande hoofdstukken al meer of minder uitgebreid behandeld. Het zijn:[10]

1. De toegenomen rekenkracht van (micro)processoren die maakt dat computers – en in toenemende mate ook mobiele apparaten – snel complexe berekeningen kunnen uitvoeren. Hierdoor konden algoritmen ineens veel meer opgaven sneller oplossen.
2. De ontwikkeling van machine learning die maakt dat computers taken kunnen uitvoeren zonder hier in detail voor te zijn geprogrammeerd. Met machine learning is er een manier gevonden om computers te laten leren van data en daarmee intelligent 'gedrag' te laten vertonen.
3. De dataficatie die maakt dat er steeds meer data beschikbaar zijn en technologische ontwikkelingen die maken dat data goedkoop kunnen worden opgeslagen. Hierdoor was er de grondstof om computers intelligentie te laten ontwikkelen.

Maar: wat is AI nu eigenlijk? De meest bondige definitie is van Margaret Boden: 'Artificial intelligence seeks to make computers do the sorts of things that minds can do.'[11] Wetenschapsjournalist Bennie Mols hanteert een enigszins vergelijkbare definitie: AI gaat over machines die dingen doen die intelligentie zouden vereisen als mensen ze zouden doen.[12] Het is van belang om bij deze definities te benadrukken dat dit cognitieve intelligentie of een cognitief vermogen betreft. Kenmerkend voor een cognitief vermogen is dat er op basis van het verwerken van binnenkomende gegevens tot een conclusie of een actie wordt gekomen.[13] De mens beschikt over veel meer vormen van intelligentie, waaronder emotionele en sociale intelligentie.[14] We moeten er dus voor

9 Zie ook Ganesan 2022.
10 Ganesan 2022; Hazenberg 2019; Maggiori 2023; Stephenson 2018; WRR 2021a.
11 Boden 2018: 1.
12 Mols 2023.
13 Koolstra, De Veer & Veltman 2021.
14 Mols 2023.

waken dat we intelligentie niet verschralen tot waar computers goed in zijn (zie ook het slot van dit hoofdstuk).[15]

Artificiële intelligentie als technologie

AI is geen concrete, afgebakende technologie. Het is een omvangrijk domein van technologieën en methoden dat zich niet zo gemakkelijk laat ordenen. In de literatuur over AI zijn uiteenlopende ordeningen te vinden. In deze paragraaf behandel ik enkele hoofdlijnen zonder de pretentie te hebben volledig te zijn en veel diepgang (aan) te brengen. Achtereenvolgens wordt ingegaan op de subdomeinen binnen AI, de leermethoden en de modellen of typen algoritmen.

AI bestaat in de eerste plaats uit een aantal subdomeinen. Dit betreft onder andere *computer vision*, *natural language processing* (NLP) en robotica. Computer vision is gericht op het vermogen van computers om beelden en objecten te herkennen, zoals aangeven wat er op een digitale afbeelding staat en het identificeren van objecten in videodata. NLP houdt zich bezig met het vermogen van computers om menselijke taal te analyseren, te begrijpen en te creëren. Chatbots en virtuele assistenten maken gebruik van NLP, maar denk ook aan spraakherkenning, automatische vertalingen en sentimentanalyse. Robotica heeft betrekking op het ontwerp, de ontwikkeling en het functioneren van robots. Het gaat dan in het bijzonder om intelligente robots, die hun omgeving observeren en daarop reageren, zoals zorgrobots of een industriële robot.[16]

Het is van belang te benadrukken dat er binnen deze subdomeinen ook gebruik wordt gemaakt van andere wetenschapsgebieden dan AI, bijvoorbeeld linguïstiek (NLP) en mechanica (robotica).

Binnen de verschillende subdomeinen speelt machine learning een centrale rol. Anders gezegd: machine learning is de drijvende kracht achter AI.[17] Het is daarom van belang om – voortbouwend op het vorige hoofdstuk – nader in te gaan op machine learning.

> *'Machine learning (ML) is about helping computers learn patterns from data with limited human intervention, By learning these patterns, the next time the computer sees something similar, it knows what decision to make.'*[18]

15 Zie hiervoor onder andere de (kritische) artikelen van Siri Beerends, bijvoorbeeld: https://www.nrc.nl/nieuws/2023/06/08/gereduceerd-tot-het-eeuwige-hulpje-van-ai (voor het laatst geraadpleegd op 22 juni 2023). Beerends wijst er onder andere op dat de grote technologiebedrijven er – vanuit economische oogpunt – belang bij hebben om intelligentie te verschralen tot wat computers goed kunnen. Zie ook het artikel van Naomi Klein in *the Guardian* waarin ze betoogt dat de maatschappelijke betekenis van AI beperkt blijft zolang AI wordt geëxploiteerd vanuit het huidige economische (kapitalistische) model. Zie https://www.theguardian.com/commentisfree/2023/may/08/ai-machines-hallucinating-naomi-klein (voor het laatst geraadpleegd op 29 juni 2023).

16 Er zijn ook softwarerobots die digitale taken automatiseren. Dit wordt Robotic Process Automation (RPA) genoemd. Binnen RPA wordt gebruikgemaakt van zowel regel-gebaseerde intelligentie als AI (zie hoofdstuk 4 voor het onderscheid). Zie Ganesan 2022.

17 Ganesan 2022.

18 Ganesan 2022: 20.

Machine learning is in essentie een (zeer) geavanceerde vorm van statistiek waarin het identificeren en gebruiken van patronen in data centraal staat.[19] Deze patronen worden gebruikt om uitspraken te doen (beslissingen te nemen) over data die het systeem nog niet heeft gezien. Dit is in essentie een vorm van voorspellen, al moet voorspellen dan breed worden opgevat (voorspellen wat er op een afbeelding staat, voorspellen van een reeks van woorden et cetera).[20] De term 'machine learning' doet misschien vermoeden dat een computer c.q. programma volledig zelfstandig leert. Dit is echter niet het geval. De mens hoeft het algoritme of model niet te programmeren – vandaar de zinsnede 'with limited human intervention' in voorgaande definitie – maar moet de computer wel in meer of mindere mate sturen in het leren. Om dit te verhelderen, gebruik ik opnieuw het voorbeeld van risicotaxatie op het gebied van recidive (zie hoofdstuk 4).[21] De programmeur of datawetenschapper geeft het systeem een set wiskundige instructies of regels – ook wel model of template genoemd – aan de hand waarvan het systeem verbanden moet leggen. Het systeem moet vervolgens een grote hoeveelheid (bewerkte) data verwerken. Op basis van de trainingsdata en de instructies leert het systeem de relaties kennen tussen de kenmerken van de data over de veroordeelden en de uitkomst (wel/geen recidive). Deze correlaties worden gebruikt om te komen tot het algoritme dat recidive gaat voorspellen. Hierbij heeft de datawetenschapper de mogelijkheid om het algoritme bij te stellen. Deze mogelijkheden zijn afhankelijk van het type algoritme.

Datawetenschap

Als gevolg van de ontwikkelingen die in de voorgaande hoofdstukken zijn beschreven, is er aan het begin van dit nieuwe millennium – op het snijvlak van wiskunde en informatica – een nieuw interdisciplinair vakgebied ontstaan: datawetenschap (*data science*).[22] Het doel van datawetenschap is om besluitvorming te baseren op dan wel te ondersteunen met inzichten die zijn geëxtraheerd uit grote hoeveelheden data.[23] Binnen dit brede kader vallen uiteenlopende subdisciplines, waaronder data mining en machine learning. Binnen het vakgebied van datawetenschap zijn in de afgelopen vijftien jaar nieuwe functionarissen ontstaan – zoals datawetenschappers en data engineers – die bedrijven, overheden en onderzoeksinstituten helpen om optimaal gebruik te maken van datawetenschap in het algemeen en AI in het bijzonder (zie ook hoofdstuk 23).[24] Vooral de functie van datawetenschapper is populair geworden. Dit is onder andere te danken aan het be-

19 Agrawal, Gans & Goldfarb 2022: 41.
20 Zie o.a. Agrawal, Gans & Goldfarb (2022) over voorspellen als essentie van AI.
21 Zie hiervoor Hordijk & Lindsen 2023.
22 Zie o.a. Beaulieu & Leonelli 2022; Kelleher & Tierney 2018.
23 Kelleher & Tierney 2018.
24 Koolstra, De Veer & Veltman 2021.

kende tijdschrift *Harvard Business Review* dat in 2012 de baan van datawetenschapper betitelde als 'the sexiest job of the 21st century'.[25]

Hoe leren computers van data? Er zijn verschillende methoden die kunnen worden gebruikt.[26] De drie belangrijkste methoden zijn *supervised learning, unsupervised learning* en *reinforcement learning*.[27] Bij supervised learning leert het systeem van data met uitkomsten die worden meegegeven. Deze uitkomsten worden ook wel gelabelde data genoemd. Op basis van de uitkomsten kan het systeem bepalen wat de belangrijkste eigenschappen van de invoerdata zijn die tot uitkomsten leiden (patronen: correlatie). Als de software voldoende voorbeelden heeft geanalyseerd, creëert het een model. Als het model is bepaald, kan het algoritme op basis van invoerdata de uitvoerdata voorspellen. Deze leermethode wordt ook gebruikt voor AI risicotaxatie-instrumenten op het gebied van onder andere recidive (zie de eerdere alinea). Op dit moment maakt het overgrote deel van de AI-toepassingen gebruik van supervised learning.[28] Bij unsupervised lerning heeft het systeem geen uitkomsten op basis waarvan eigenschappen kunnen worden bepaald. Het systeem zoekt zelfstandig naar patronen en structuren in de data. Bijvoorbeeld: op basis van allerlei data over financiële transacties kan een systeem leren afwijkende transacties te herkennen ten behoeve van opsporing van fraude. Het label 'afwijkend' is dan niet vooraf gegeven, maar wordt op basis van de data gecreëerd. Het voordeel hiervan is dat er in mindere mate menselijke kennis wordt gereproduceerd en er (meer) verrassende inzichten kunnen ontstaan. Unsupervised learning is echter – in vergelijking met supervised learning – voor een beperkter aantal taken bruikbaar.[29] Anders gezegd: met niet-gelabelde data is minder mogelijk dan met gelabelde data. Unsupervised learning wordt in veel gevallen dan ook gebruikt om het probleem van niet gelabelde datasets te omzeilen.[30] Tot slot: reinforcement learning. Deze methode verschilt wezenlijk van de hiervoor behandelde leermethoden. Bij reinforcement learning leert de computer via trail-and-error. Het systeem krijgt een taak, wordt in een (virtuele) omgeving gezet en gaat daarin handelen (beslissingen nemen). Op basis van het handelen krijgt het systeem feedback. Het krijgt een beloning of straf. Reinforcement learning is moeilijk toe te passen en is dan (vooralsnog) ook de minst gebruikte leermethode van de drie leermethoden die zijn behandeld.[31]

Dan de modelklassen of typen algoritmen.[32] Voorbeelden hiervan zijn lineaire modellen, beslisbomen en neurale netwerken. Deze zijn vaak verbonden aan de leermethoden, maar dit hoeft niet. Zo wordt bij een beslisboom vaak gebruikgemaakt van super-

25 Thamm, Gramlich & Borek 2020.
26 Deze toelichting is vooral gebaseerd op Koolstra, De Veer & Veltman 2021; Mannens 2021; Thamm, Gramlich & Borek 2020.
27 Zie voor andere leermethoden o.a. Mannens 2021.
28 Mannens 2021; Thamm, Gramlich & Borek 2020.
29 Maggiori 2023; Thamm, Gramlich & Borek 2020.
30 Thamm, Gramlich & Borek 2020.
31 Ganesan, 2022; Thamm, Gramlich & Borek 2020.
32 Deze paragraaf is gebaseerd op Koolstra, De Veer & Veltman 2021; Thamm, Gramlich & Borek 2020.

vised learning, terwijl bij neurale netwerken alle leermethoden worden gebruikt (al is supervised learning wel dominant). Ik beperk de uitwerking tot neurale netwerken, omdat dit de categorie modellen is die in de afgelopen periode voor doorbraken in de toepassing van AI heeft gezorgd.[33] Een neuraal netwerk bestaat uit filters of knooppunten die elk een berekening uitvoeren op basis van inputdata en het vervolgens doorgeven aan een ander filter. Een input beweegt zich zo door het netwerk en dit leidt uiteindelijk tot een uitkomst (vaak een vorm van voorspelling). Tussen de input en output bevinden zich vaak verschillende lagen met filters. In dit verband wordt de term 'diep' gebruikt. Het trainen van een dergelijk diep neuraal netwerk heet *deep learning*. Een neuraal netwerk kan – in vergelijking met andere modelklassen – relatief complexe taken uitvoeren en is daarom ook zo populair.[34] Een voorbeeld van een complexe taak is beeldherkenning. Hierna een uitgebreid voorbeeld dat is bedoeld om het concept van een neuraal netwerk te verhelderen.[35]

Deep learning voor het herkennen van afbeeldingen

Stel dat je instructies schrijft om een computer te vertellen of er op een foto wel of geen hond staat. Je zou kunnen beginnen met de voor de hand liggende zaken: als het vier poten heeft, als het slappe oren heeft, als het een vacht heeft, enzovoort. Maar wat moet je met de foto's van een zittende hond? Of de foto's waarop je niet alle poten kunt zien? Wat moet je met de honden met puntoren? Of gespitste oren? Of de honden die niet naar de camera kijken? En hoe ziet 'vacht' er anders uit dan pluizig tapijt? Of de wol van een schaap? Of gras. Je zou dit natuurlijk allemaal in extra instructies kunnen opnemen, en alle mogelijke soorten hondenoren of hondenvacht of zittende posities kunnen doornemen, maar binnen de kortste keren zal je algoritme zo'n enorme omvang hebben dat het volkomen onwerkbaar wordt, en dan ben je nog niet eens begonnen met onderscheid maken tussen honden en andere vierpotige dieren met een vacht. Je moet een andere manier zien te vinden. De truc is om af te stappen van het op regels gebaseerde algoritme en iets te gebruiken dat een 'neuraal netwerk' wordt genoemd.

Je kunt je een neutraal netwerk voorstellen als een reusachtig wiskundig bouwsel met een heleboel knoppen en wijzers. Je stopt er een foto aan de ene kant in, hij gaat door het bouwsel heen en aan de andere kant komt er een *schatting* uit over wat er op de afbeelding staat. Een waarschijnlijkheid voor elke categorie: Hond; Geen hond. In het begin is je neurale netwerk één grote warboel. Het begint zonder kennis – zonder idee over wat wel of geen hond is. Alle knoppen en wijzers zijn willekeurig ingesteld. Het gevolg

33 Thamm, Gramlich & Borek 2020.

34 Het doorbraakmoment van neurale netwerken is ook verbonden aan een spel: in 2016 versloeg AlphaGo – een programma van DeepMind (dochteronderneming van Alphabet/Google) – 's werelds beste Go speler Lee Sedol. Go is in vergelijking met schaken en Jeopardy een heel complex spel. Zie o.a. Mols (2023) voor een beschrijving van deze gebeurtenis.

35 Dit voorbeeld is overgenomen uit Fry (2018).

> is dat de antwoorden een ratjetoe zijn – in deze toestand zou het een afbeelding nog niet accuraat kunnen herkennen. Maar met elke foto die je erin stopt, stel je de die knoppen en wijzers fijner af. Langzamerhand train je het. Je afbeelding van een hond wordt erin gestopt. Na elke schatting die het netwerk doet, gaat een verzameling wiskundige regels aan de slag om alle knoppen aan te passen tot de voorspelling dichter bij het juiste antwoord komt. Vervolgens stop je er nog een afbeelding in, en nog een, en verfijn je het zo elke keer dat het iets mis heeft; verstevig je de paden via de opeenvolging van knoppen die tot succes leiden en laat je de paden die tot mislukking leiden verdwijnen. Informatie over wat de ene foto van een hond op de andere doet lijken, verspreidt zich achterwaarts door het netwerk. Dit gaat door – nadat er honderden en duizenden foto's zijn ingevoerd – tot het netwerk niets meer mis heeft. Uiteindelijk kun je het een afbeelding laten zien die het nog nooit heeft gezien en zal het in staat zijn je met een hoge graad van nauwkeurigheid te zeggen of er wel of geen hond op de foto staat.

Diepe neurale netwerken zijn op dit moment de hype in het domein van AI. Dit komt onder andere doordat deze modellen worden gebruikt binnen een toepassingsgebied – je kunt het (ook) beschouwen als een subdomein – dat generatieve AI wordt genoemd. Generatieve AI is een snelgroeiend gebied binnen AI dat wordt gekenmerkt door het creëren (genereren) van nieuwe, synthetische media, waaronder tekst, afbeeldingen en video's.[36] Het inmiddels meest bekende voorbeeld van generatieve AI is ChatGPT.[37] *GPT* staat voor *generative pretrained transformer*. Dit wil zeggen dat ChatGPT een basismodel is dat is 'voor getraind' op zeer omvangrijke datasets. Dit betreft in het bijzonder data in de vorm van tekst van het internet, digitale boeken en ondertiteling van video's. Het wordt daarom ook wel een 'large language model' (LLM) genoemd.[38] Dit model is in staat om natuurlijke taal te begrijpen en te produceren en kan onder andere worden ingezet voor het maken van teksten, samenvatten van teksten, beantwoorden van vragen en schrijven van computercodes. Er wordt gebruikgemaakt van een algoritme met miljarden parameters. Het gegeven dat het model voor meerdere taken kan worden ingezet, maakt dat het ook wel *general purpose AI* wordt genoemd.[39] Als gebruiker kun je opdrachten (prompts) geven aan een chatbot en met de chatbot interacteren. Door gebruik te maken van zogenaamde *transformers* is de computer in staat om de context van zinnen te begrijpen en kan die een gesprek met een

36 Binnen de generatieve AI zijn twee technieken dominant, namelijk een *generative adversarial network* (GAN) en *variational autoencoder* (VAE). Dit zijn andere typen diep neurale netwerken dan de conventionele diep neurale netwerken. Zie voor een toelichting o.a. Mannens 2021 en Foster 2023.

37 Er zijn ook diverse applicaties om afbeeldingen te genereren, zoals Midjourney en DALL-E (van hetzelfde bedrijf als ChatGPT).

38 ChatGPT is op dit moment het bekendste voorbeeld van een LLM. Alle bedrijven die onderdeel zijn van 'Big tech' zijn bezig met de ontwikkeling van LLM. Zo is Google bezig met Bard, Apple met een taalmodel dat Ajax wordt genoemd en Meta met LLama 2.

39 Dit is heel iets anders dan algemene AI. Zie het slot van dit hoofdstuk.

gebruiker voeren.[40] Het onderliggende model wordt gebruikt in veel meer toepassingen – zoals Microsoft Bing – en is in staat om steeds meer taken uit te voeren.[41] De introductie van ChatGPT heeft veel stof doen opwaaien en heeft de hype rondom AI in behoorlijke mate gevoed.[42] Het wordt door sommigen ook wel vergeleken met 'het iPhone-moment'.[43] Waar de iPhone de doorbraak van de smartphone representeert, staat de introductie van ChatGPT voor de doorbraak van AI. Naast enthousiasme over de mogelijkheden van ChatGPT werden en worden er ook de nodige kritische geluiden en zorgen geuit, waaronder desinformatie, (grootschalige) inbreuk op auteursrechten en misbruik door criminelen. In het vervolg van dit boek komt een deel van deze kwesties aan de orde.

Impact en ontwikkeling van artificiële intelligentie

AI is uitgegroeid tot een van de grootste technologische innovaties die de wereld aan het veranderen is.[44] Er wordt vanuit gegaan dat er sinds het begin van de digitale revolutie – nu zo'n zestig jaar geleden – geen technologie is geweest met zoveel consequenties voor (onder andere) de uitvoering van werk in organisaties.[45] AI vergroot het menselijke vermogen tot waarnemen, begrijpen en leren.[46] Dit heeft onder andere gevolgen voor de wijze waarop (cognitieve) taken binnen organisaties worden uitgevoerd.[47] AI leidt in de eerste plaats tot het *automatiseren* van taken.[48] Dit betreft vooralsnog vooral afgebakende taken, bijvoorbeeld het analyseren van data om de ontwikkeling van de koersen van aandelen te voorspellen en op basis hiervan beslissingen te nemen. AI is bovenmenselijk goed in het uitvoeren van dit soort 'smalle' taken. Er liepen op de New York Stock Exchange 5500 beurshandelaren rond. Nu zijn dat er minder dan 400 en zijn veel werkzaamheden overgenomen door AI.[49] Er zijn echter ook (cognitieve) taken die een minder afgebakend karakter hebben en in mindere mate door middel van software kunnen worden uitgevoerd. Deze taken vinden veelal ook in een meer dynamische c.q. veranderlijke omgeving plaats met (dus) meer onze-

40 De voorgaande zinnen vormen de toelichting op de term 'ChatGPT'.

41 Enkele maanden na ChatGPT 3 kwam ChatGPT 4 uit. ChatGPT 4 is onder andere in staat om zowel teksten als afbeeldingen als invoer te begrijpen. Hierdoor heeft het basismodel van ChatGPT zich in feite ontwikkeld van een LLM naar een large multimodal model.

42 De verwachting is dat het gebruik van generatieve AI in het bedrijfsleven vanaf 2023 een vlucht gaat nemen. Zie bijvoorbeeld: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year (voor het laatst geraadpleegd op 15 augustus 2023).

43 https://www.trouw.nl/opinie/de-schrijfapp-spreekt-niet-altijd-de-waarheid (voor het laatst geraadpleegd op 2 januari 2023).

44 Koolstra, De Veer & Veltman 2021; Davenport & Mittal 2023.

45 Waardenburg, Huysman & Agterberg 2020.

46 Daugherty & Wilson 2018.

47 Borek & Prill 2020.

48 Wanneer het automatiseren van taken breed wordt opgevat, dan betreft het ook de inzet van virtuele personen c.q. avatars. Hierbij kan worden gedacht aan India waar virtuele nieuwslezers worden ingezet. Inmiddels maken acteurs in Hollywood zich ook zorgen over de impact van generatieve AI op hun werk. Zie https://www.universiteitleiden.nl/nieuws/2023/07/staking-in-hollywood-is-ai-echt-een-bedreiging-voor-acteurs (voor het laatst geraadpleegd op 1 augustus 2023).

49 Yang 2020.

kerheid.[50] Het automatiseren van taken met behulp van AI is in die omstandigheden niet mogelijk. AI kan dan echter (veelal) wel een rol spelen in het *versterken* of aanvullen van het menselijke vermogen bij de uitvoering van taken. Hierbij kan onder andere worden gedacht aan ondersteuning bij medische diagnoses.
Het is van belang te benadrukken dat de AI die er nu is (dus) een smal of gericht karakter heeft.[51] AI kan één taak – waarvoor het getraind is met voorbeelden uit het verleden – snel en accuraat uitvoeren, bijvoorbeeld diagnose van borstkanker op basis van analyse van duizenden mammografieën. Hierbij heeft iedere taak een eigen model.[52] AI kan geen taken uitvoeren die een breed begrip van de wereld vragen.[53] AI is daarmee ook niet te vergelijken met algemene, menselijke intelligentie.[54] In het domein van de generatieve AI zijn er inmiddels toepassingen die voor verschillende taken kunnen worden ingezet. Dit impliceert dat AI meer generieke capaciteiten krijgt, maar dit is nog heel iets anders dan artificiële, algemene intelligentie (AGI).[55] De hype rondom generieke AI heeft als risico dat we ons laten meeslepen in onrealistische narratieven.[56] Ook moet worden beseft dat de huidige AI (heel) veel meer voorbeelden (dan de mens) nodig heeft om te leren.[57] Een kind van twee of drie jaar hoeft maar een paar keer een mier te zien en bestuderen om in het vervolg te weten dat een mier een mier is. AI heeft daar talloze voorbeelden voor nodig en leert dan ook op fundamenteel andere wijze dan een mens. Het ziet geen mier, maar analyseert heel veel pixels tegelijkertijd (zie ook hoofdstuk 3 over digitale data). Menselijke intelligentie is daarnaast ook veel meer dan (statistische) patroonherkenning (zie ook het begin van dit hoofdstuk).[58]

Het voorgaande heb ik opgenomen ten behoeve van het realiteitsbesef en niet om de potentie van AI te bagatelliseren.[59] AI heeft in de afgelopen tien jaar een spectaculaire

50 Zie o.a. Gigerenzer 2022.
51 In het Angelsaksisch wordt de term 'narrow AI' gebruikt. Smalle AI kan echter 'klein' of 'beperkt' klinken en doet daarmee geen recht aan waar het voor staat (zie ook Ganesan, 2022). Daarom heeft 'gerichte AI' mijn voorkeur.
52 Maggiori 2023.
53 Maggiori 2023; Mols 2023.
54 Ganesan 2022.
55 Artificiële, algemene intelligentie (AGI) – een vorm van AI die vergelijkbaar is met de brede intellectuele taken die een mens kan begrijpen en leren – is vooralsnog een theoretisch concept waarvan het onzeker is of het kan worden gerealiseerd. De huidige methodologie van machine learning zal in ieder geval niet zomaar leiden tot artificiële, algemene intelligentie (zie Maggiori, 2023). Er zijn fundamentele innovaties of doorbraken nodig voor het realiseren van artificiële, algemene intelligentie (AGI). Zie hiervoor: Mols 2023.
56 Deze narratieven leiden – zo wordt door verschillende experts opgemerkt – af van de werkelijke risico's van de wijze waarop AI zich nu ontwikkelt, zoals verdere machtsconcentratie bij technologiebedrijven, massasurveillance en grootschalige verspreiding van desinformatie (zie ook hoofdstuk 9). Zie onder andere https://www.parool.nl/columns-opinie/opinie-problemen-gevaren-en-ethische-uitdagingen-ai-urgenter-dan-vermeende-superintelligentie (voor het laatst geraadpleegd op 5 juli 2023). Zie ook de eerdere verwijzing naar het artikel van Naomi Klein.
57 Vooral voor neurale netwerken geldt dat ze 'datahongerig' zijn. Dit heeft ook als gevolg dat AI in het algemeen en het ontwikkelen van neurale netwerken in het bijzonder met veel energieverbruik gepaard gaat. De ecologische gevolgen van AI vormen een apart thema dat ik hier niet verder behandel.
58 Mols 2023.
59 Hierbij moet worden opgemerkt dat er tegen de potentie van AI verschillend wordt aangekeken. Er is eigenlijk geen eenduidig verhaal te vertellen over AI (zie Bouteca et al., 2020).

ontwikkeling doorgemaakt en ontwikkelt zich in een rap tempo.[60] Hierbij moet worden opgemerkt dat er inmiddels weliswaar sprake is van brede adoptie in de samenleving, maar de ontwikkeling van (gerichte) AI staat nog in de kinderschoenen. 'Even though AI seems everywhere, like many other breakthrough technologies before, it is only just getting started.'[61] De huidige tijd wordt ook weleens gedefinieerd als de *between times*: na de doorbraak van de technologie, maar voor de benutting van diens 'ware' potentieel.[62] Anders gezegd: we zijn de mogelijkheden van AI nog maar net aan het ontdekken.[63] De ervaringen met eerdere systeemtechnologieën leren dat het tijd kost alvorens het potentieel van de technologie wordt waargemaakt. Wat buiten kijf staat, is dat mens en machine – in de verdere ontwikkeling van AI – steeds meer met elkaar verweven raken.[64] Dit zal van invloed zijn op de fenomenen waarmee de politie te maken krijgt én op de wijze waarop het politiewerk wordt uitgevoerd.

60 Davenport & Mittal 2023; Mols 2023.
61 Agrawal, Gans & Goldfarb 2022: 53.
62 Agrawal, Gans & Goldfarb 2022.
63 Mols 2023.
64 Koolstra, De Veer & Veltman 2021.

Deel II Veiligheidsvraagstuk

6 Digitalisering van criminaliteit

Digitalisering is van invloed op hoe criminaliteit in de samenleving verschijnt. Hoewel traditionele criminaliteit zeker niet is verdwenen, is er door digitalisering een nieuwe hoofdcategorie van criminaliteit bijgekomen: digitale criminaliteit. Dit hoofdstuk behandelt de digitalisering van criminaliteit die heeft plaatsgevonden en op dit moment voortschrijdt. Ik ga eerst in op de (veronderstelde) *crime drop* en vervolgens op het verschijnsel 'digitale criminaliteit'.

De forse afname van de traditionele criminaliteit

Tussen 1960 en 2000 groeide het criminaliteitsprobleem in Nederland. In de geregistreerde criminaliteit in Nederland deed zich in deze periode ongeveer een vertienvoudiging[1] voor.[2] Criminaliteit werd in Nederland – en in andere *high crime societies* – in de jaren tachtig een vanzelfsprekend onderdeel van het dagelijks leven.[3] Als gevolg hiervan kwam het criminaliteitsprobleem in die periode steeds hoger op de agenda te staan.[4] Er volgde beleidsplan na beleidsplan met maatregelen om het criminaliteitsprobleem te beteugelen. Het steeds verder uitdijende pakket aan maatregelen leidde stap voor stap tot een nieuwe sector: de maatschappelijke veiligheidszorg.[5] Deze sector bestond en bestaat uit een groot aantal publieke en private partijen die samenwerken aan het voorkomen en bestrijden van allerlei vormen van ordeverstoringen, overlast, criminaliteit en andere ongewenste verschijnselen. Dit 'veiligheidsprogramma' heeft ertoe geleid dat het monopolie dat politie en justitie hadden in de aanpak van criminaliteit is doorbroken

Sinds 2002 is er sprake van een kentering: zowel de geregistreerde criminaliteit als het zelf gerapporteerde slachtofferschap zijn vanaf dat jaar fors afgenomen. De geregistreerde criminaliteit bevindt zich inmiddels op het laagste punt in bijna veertig jaar. Het slachtofferschap van delicten is tussen 2005 en 2022 met 60% procent afgenomen naar 17% van de bevolking.[6] Kortom: de kans om slachtoffer te worden van een delict is vandaag fors kleiner dan die vijftien jaar geleden was. Deze ontwikkeling wordt sterk beïnvloed door de afname van de (veelvoorkomende) vermogenscriminaliteit, die de

1 Wanneer rekening wordt gehouden met de bevolkingsgroei was er sprake van een verzevenvoudiging.
2 Boutellier 2002; Terpstra 2010b.
3 Garland 2001.
4 Boutellier 2019.
5 Terpstra 2010b.
6 Akkermans et al. 2022.

bulk vormt van de geregistreerde criminaliteit en het (gerapporteerde) slachtofferschap. Deze *crime drop* is niet uniek voor Nederland, maar is een meer algemene trend in Noord- en West-Europese landen en Angelsaksische landen.[7] Het is een robuuste tendens.[8]

De sterke daling van de criminaliteit in de westerse wereld heeft veel wetenschappelijke interesse gewekt. Sommigen spreken zelfs over een subdiscipline binnen de criminologie, gericht op het ontrafelen van de puzzel: hoe kan de crime drop worden verklaard?[9] Er is in de criminologie weliswaar discussie over het antwoord op deze vraag,[10] maar met enige voorzichtigheid kan worden gesteld dat het eerdergenoemde veiligheidsprogramma – dat vanaf het einde van de jaren tachtig tot ontwikkeling is gekomen – succes heeft gehad.[11] Simpel gesteld: de gelegenheid voor het plegen van de veelvoorkomende criminaliteit die in de tweede helft van de vorige eeuw rap toenam, is vervolgens sterk afgenomen. Burgers en bedrijven zijn steeds meer gaan investeren in allerlei preventieve maatregelen.[12] Kortom: we hebben ons aangepast aan het gegeven dat criminaliteit een vanzelfsprekend onderdeel van het dagelijks leven was geworden.

De vraag is echter: is de criminaliteit wel verdwenen of heeft het veiligheidsoffensief uit de vorige eeuw ook vooral de criminaliteit uit de vorige eeuw bestreden?

De mutatie van de traditionele criminaliteit

De afname van de geregistreerde (veelvoorkomende) criminaliteit sinds 2002 heeft parallel plaatsgevonden met de opkomst van het internet (zie hoofdstuk 2). Het internet – eerst web 1.0 en later vooral web 2.0 – heeft een omvangrijke, nieuwe gelegenheidsstructuur gecreëerd voor het plegen van criminaliteit.[13] Van deze gelegenheidsstructuur wordt in toenemende mate gebruikgemaakt.[14] De traditionele criminaliteit is gemuteerd in nieuwe digitale vormen, soms leidend tot helemaal nieuwe delicten. Dit proces van *technological-mediated criminal transference* heeft zich in eerste aanvang in belangrijke mate buiten ons gezichtsveld afgespeeld en is niet of nauwelijks meegenomen in het narratief over de verdwenen criminaliteit.[15] 'The missing element in this overall picture of the crime drop is the evolution of cybercrime.'[16] Kortom: de criminaliteit is niet verdwenen, maar heeft zich verplaatst naar het digitale domein. Dit wil overigens niet zeggen dat alle criminelen zijn overgestapt van de koevoet naar het toetsenbord, maar duidelijk is wel dat de grootschalige veranderingen in gelegenheids-

7 Smit 2020; zie ook Caneppele & Aebi 2017.
8 Boutellier 2020.
9 Voor een overzicht zie Farrall 2017; Kotzé 2019.
10 Boutellier 2020; De Koning 2017.
11 De Waard 2020; Spithoven 2020.
12 De Jong 2018; Farrell et al. 2010.
13 Boutellier 2020; Caneppele & Aebi 2017; David 2023; Stol & Strikwerda 2017.
14 Van der Wagen, Oerlemans & Weulen Kranenbarg 2020a.
15 Kotzé 2019.
16 Caneppele & Aebi 2017: 69.

structuren hebben geleid tot een gelijktijdige daling van de traditionele (offline) criminaliteit én stijging van de digitale (online) criminaliteit.[17]

De digitalisering van criminaliteit heeft geleid tot verschillende begrippen en categorieën in zowel de wetenschappelijke literatuur als de praktijk. Ik heb – op dit moment – de voorkeur voor het hoofdbegrip digitale criminaliteit met daarbinnen het onderscheid tussen cybercriminaliteit en gedigitaliseerde criminaliteit.[18] Bij cybercriminaliteit is ICT zowel middel als doelwit. Dit wordt ook wel *cyber dependent* of *target cybercrimes* genoemd.[19] Voorbeelden zijn het hacken van een database met persoonsgegevens, het platleggen van een website van een bank met een DDoS-aanval en het gijzelen van IT-systemen voor losgeld (ransomware). Gedigitaliseerde criminaliteit is criminaliteit waarbij ICT het middel is of, anders gezegd, waarbij ICT een belangrijk onderdeel van de *modus operandi* is. Dit wordt ook wel *cyber enabled* of soms *computer-gerelateerd* genoemd.[20] Een voorbeeld is online fraude of het verspreiden van kinderporno via het internet. Het zijn in de regel geen (relatief) nieuwe delicten – zoals bij cybercriminaliteit – maar de verschijningsvorm is wel (relatief) nieuw. *Old crimes, using new tricks*.[21] Bij zowel cybercriminaliteit als gedigitaliseerde criminaliteit staat ICT in meer of mindere mate centraal als doel en/of middel. Er wordt soms ook nog onderscheid gemaakt in een derde categorie waarbij ICT een onderdeel is van de modus operandi van een delict.[22] Het delict wordt dan niet mogelijk gemaakt door ICT, maar er wel in meer of mindere mate door gefaciliteerd.[23] Een voorbeeld hiervan is het gebruik van versleutelde communicatie tussen criminelen of het gebruik van online *dark markets* (zie ook hoofdstuk 7). Het nadeel van deze derde categorie is dat hierdoor steeds meer vormen van criminaliteit als digitale criminaliteit zijn te beschouwen, omdat het gebruik van ICT bij het plegen van criminaliteit gemeengoed is.[24] Het heeft daarom mijn voorkeur om digitale criminaliteit te beperken tot gedigitaliseerde criminaliteit en cybercriminaliteit.

Het is niet gemakkelijk om de precieze omvang van digitale criminaliteit in kaart te brengen. Dit heeft verschillende redenen, zoals de geringe mate waarin aangifte wordt gedaan en de wijze waarop de politie gedigitaliseerde criminaliteit registreert.[25] Duidelijk is wel dat digitale criminaliteit een steeds groter aandeel vormt van de totale criminaliteit.[26] Inmiddels is tussen de 15 en 20% van de bevolking jaarlijks slachtoffer

17 Spithoven 2020.
18 Er wordt in dit verband ook gebruikgemaakt van het onderscheid tussen cybercriminaliteit in ruime zin (= digitale criminaliteit) en cybercriminaliteit in enge zin (= cybercriminaliteit). Zie bijvoorbeeld Van der Wagen, Oerlemans & Weulen Kranenbarg 2020a.
19 Schermer 2022.
20 Leukfeldt, Notté & Malsch 2018; Schermer 2022.
21 Holt, Bossler & Seigfried-Spellar 2022: 535.
22 Van den Eeden et al. 2021; zie ook Wall 2007.
23 Zie ook Schermer 2022.
24 Zie ook Van den Eeden et al. 2021.
25 Van der Wagen, Oerlemans & Weulen Kranenbarg 2020b; Van de Weijer, Leukfeldt & Van der Zee 2020.
26 Beerthuizen, Sipma & Van der Laan 2020; Spithoven 2020.

van vooral gedigitaliseerde criminaliteit. Het gaat dan in het bijzonder om allerlei vormen van online oplichting.[27] Naast daadwerkelijk slachtofferschap heeft een groot deel van de bevolking te maken gehad met een (vermoedelijke) poging tot online oplichting door middel van een telefoontje, e-mail of ander bericht.[28] Kortom: het slachtofferschap neemt door de bank genomen toe. Ook wordt steeds duidelijker dat digitale criminaliteit bij een deel van de slachtoffers leidt tot emotionele of psychische problemen, al dan niet veroorzaakt door financiële schade.[29] Tevens valt op dat een toenemend aantal jongeren betrokken is bij het plegen van digitale criminaliteit.[30] Dit betreft uiteenlopende jongeren: van jongeren die ICT-onderwijs volgen en weleens digitale criminaliteit plegen[31] tot jongeren die zich voorheen bezighielden met straatcriminaliteit en hun activiteiten hebben verlegd naar het digitale domein.

De F-game: jongeren en online fraude en oplichting[32]

Wetenschappelijke studies en onderzoeksjournalistiek laten zien dat jongeren die zijn ingebed in de straatcultuur hun werkterrein hebben verplaatst van de fysieke straat naar de digitale straat. Dit komt onder andere tot uiting in (specifieke) Telegram-groepen waarin jongeren informatie en diensten uitwisselen voor het plegen van digitale criminaliteit. Hierbij kan worden gedacht aan het vragen of aanbieden van creditcardgegevens, bankpassen en methoden om geld afkomstig van onder andere phishing-aanvallen te gebruiken. In deze online interacties wordt gebruikgemaakt van specifieke (straat)taal. De criminaliteit waar het veelal over gaat, wordt gedefinieerd als de 'F-game': online fraude (wat dus als een spel wordt omschreven). Men zoekt bijvoorbeeld 'leads': gegevens van personen met een mobiele telefoon die kunnen worden benaderd met 'nepberichten' van bijvoorbeeld een bank. Of 'lebbers':[33] mensen die in een crimineel callcenter de leads nabellen en hierbij een script gebruiken. Als iemand hapt, wordt het geld afhandig gemaakt en door 'bonkers' op bankrekeningen gestort van zogenaamde 'zwaaiers' en 'nippers'. Dit zijn geldezels die hun bankrekeningnummer beschikbaar stellen en bij het pinautomaat het geld uit de muur halen.[34] Hierbij wordt niet zelden gebruikgemaakt van kwetsbare personen, die het meest

27 Akkermans et al. 2022; Akkermans et al. 2023.
28 Akkermans et al. 2022.
29 Zie hiervoor Akkermans et al. 2023. Er is overigens nog weinig wetenschappelijk onderzoek gedaan naar slachtoffers van digitale criminaliteit.
30 https://nos.nl/artikel/2456322-jongeren-vaker-betrokken-bij-fraude-en-cybercrime-politie-maakt-zich-zorgen (voor het laatst geraadpleegd op 3 januari 2023).
31 Weulen Kranenbarg, Van der Toolen & Weerman 2022.
32 Zie Roks & Monshouwer 2020; Verlaan 2020. Zie ook: https://www.parool.nl/amsterdam/makkelijk-en-zonder-veel-risico-hoe-online-fraudeurs-uit-amsterdam-zuidoost-miljoenen-binnenharken-met-f-game (voor het laatst geraadpleegd op 21 februari 2023). En: https://ccv-secondant.nl/platform/article/de-criminele-kosten-en-baten-van-online-fraude (voor het laatst geraadpleegd op 1 augustus 2023).
33 In straattaal worden woorden geregeld omgekeerd geschreven (zie Roks & Monshouwer, 2020).
34 Uit kwantitatief onderzoek onder 3.000 jongeren blijkt dat 10% is benaderd om een rol als geldezel te vervullen (Bekkers et al. 2023). Men wordt vooral benaderd via sociale media (Snapchat, Instagram) en vindt het ook 'vrij normaal' om te worden benaderd. Ongeveer 1% geeft aan als geldezel te hebben gefungeerd.

risico lopen, omdat zij traceerbaar zijn. Zij dragen dat geld af aan de 'creamers', die gemakkelijker anoniem blijven. Dergelijke straattaal op het gebied van digitale criminaliteit is niet alleen te observeren in Telegram-groepen, maar is ook te beluisteren in rapmuziek waarin wordt opgeschept over de gepleegde criminaliteit ('We klemmen die CC, dan gaan we shoppen!').

Met betrekking tot cybercriminaliteit kan worden geconstateerd dat de zware, georganiseerde cybercriminaliteit in de afgelopen jaren qua slachtoffers, schade en criminele opbrengsten een industriële omvang heeft aangenomen.[35] De digitale kwetsbaarheid van bedrijven en instellingen wordt benut door cybercriminele groepen die aan de lopende band aanvallen uitvoeren, waaronder een groeiend aantal ransomware-aanvallen.[36] Cybercriminaliteit heeft een aantrekkelijke *businesscase*: potentieel hoge opbrengsten en een relatief lage pakkans (zie ook het vervolg van dit hoofdstuk).[37] Gestolen data spelen een sleutelrol in veel vormen van cybercriminaliteit.[38] Ze zijn zowel middel in de uitvoering van delicten als opbrengst van delicten.[39] Cyberaanvallen kunnen vergaande gevolgen hebben, waaronder omvangrijke economische schade[40] en het bedreigen van de continuïteit van vitale processen in de samenleving en zijn daarmee een risico voor de nationale veiligheid.[41] Naast delicten die worden gepleegd door cybercriminele groepen zijn er statelijke actoren die via cyberspace de nationale veiligheid bedreigen door sabotage van de vitale infrastructuur en het (via onder andere desinformatie) onder druk zetten van de cohesie in de Nederlandse samenleving.[42] Steeds meer landen ontdekken internet als wapen en hebben offensieve cyberprogramma's. 'Zoals eens met kernwapens is er nu een wapenwedloop gaande waarvan niemand weet waar die eindigt', aldus Huib Modderkolk in *Het is oorlog maar niemand die het ziet*.[43] De dreiging voor Nederland komt vooral, maar zeker niet alleen, uit Rusland en China. Door verharding van de geopolitieke situatie – in het bijzonder de oorlog in Oekraïne – neemt de dreiging van statelijke actoren die cyberaanvallen uitvoeren (verder) toe.[44]

35 NCTV 2022a.
36 Hierbij wordt kwaadaardige software via een beveiligingslek geïnstalleerd om daarmee de toegang tot het computersysteem of bestanden op het systeem te versleutelen. Er wordt vervolgens losgeld – vaak in virtuele valuta (zie hoofdstuk 7) – geëist voor het ontsleutelen ervan. Zie ook Van der Voort & Warnaars (2020).
37 Schermer 2022; zie ook NCTV 2023.
38 Dit geldt overigens ook voor gedigitaliseerde criminaliteit. Zie ook het kader over de 'F-game'.
39 Europol 2023b.
40 Uit onderzoek van IT-beveiliger ESET blijkt dat een cyberaanval c.q. -incident een mkb-bedrijf gemiddeld zo'n 270.000 euro kost. Twee derde van de ondervraagde bedrijven heeft te maken gehad met een cyberaanval. Een cyberaanval kan leiden tot dan wel bijdragen aan faillissement. Zie onder andere https://www.bnr.nl/nieuws/technologie/10494716/cybercrime-kost-bedrijfsleven-veel-meer-dan-in-andere-landen (voor het laatst geraadpleegd op 10 juli 2023).
41 Europol 2021a; NCTV 2022a.
42 Zie hiervoor het Dreigingsbeeld Statelijke Actoren 2 van de AIVD, MIVD en NCTV van 2022.
43 Modderkolk 2019.
44 Europol 2023b; NCTV 2023.

Digitale criminaliteit is anders dan de politie gewend is

De digitalisering van criminaliteit heeft ervoor gezorgd dat het criminaliteitsbeeld in Nederland in het afgelopen decennium fundamenteel is veranderd.[45] Digitale criminaliteit is de nieuwe veelvoorkomende criminaliteit geworden.[46] Digitale criminaliteit heeft zich tevens vermengd met georganiseerde criminaliteit (zie hoofdstuk 7).[47] Voor een deel van de criminele groepen is digitale criminaliteit een markt erbij waarin veel te verdienen valt.

Het fundamentele karakter van de verandering schuilt niet alleen in het gegeven dat de criminaliteit is getransformeerd, maar ook en misschien wel vooral in het gegeven dat digitale criminaliteit geen 'oude wijn in nieuwe zakken' is.[48] Het is een nieuw type criminaliteit dat op een aantal punten wezenlijk afwijkt van de traditionele criminaliteit: digitale criminaliteit heeft andere kenmerken dan traditionele criminaliteit. Dit wordt veroorzaakt door het domein waarop digitale criminaliteit zich grotendeels afspeelt: het internet. Ik behandel de vijf belangrijkste kenmerken op hoofdlijnen.

Digitale criminaliteit is tot op zekere hoogte de-territoriaal.[49] Dit wil onder andere zeggen dat de locaties van dader(s) en slachtoffer(s) veelal niet in elkaars nabijheid liggen.[50] Dit is zichtbaar binnen Nederland – bijvoorbeeld bij vriend-in-noodfraude waarbij slachtoffers en dader(s) in de regel ver uit elkaar wonen[51] – maar zeker ook in internationaal verband. Nederland is vanwege de uitstekende internet-infrastructuur aantrekkelijk voor internationaal opererende cybercriminele groepen. Ons land wordt gezien als een vrijhaven voor datapakketjes.[52] Nederlandse datacentra zijn bijvoorbeeld betrokken bij allerlei vormen van cybercriminaliteit, via uiteenlopende *resellers*[53] en hun klanten.[54] De resellers en klanten bevinden zich vaak in het buitenland. De criminelen zitten dan in het buitenland op hun muis te klikken, terwijl bijvoorbeeld de ransomware vanuit Nederland wordt gepusht naar computers van slachtoffers of kinderporno wordt verspreid.[55] Kortom: vanaf Nederlandse servers gaat een hoop rot-

45 Boutellier 2019; Spithoven 2020.
46 Leukfeldt 2018.
47 https://www.om.nl/actueel/nieuws/2022/10/18/openbaar-ministerie-traditionele-misdaad-en-cybercriminaliteit-smelten-steeds-meer-samen (voor het laatst geraadpleegd op 2 januari 2023).
48 Van der Wagen 2018. Zie David (2023) voor een uitgebreide behandeling van de vraag of er sprake is van oude wijn in nieuwe zakken.
49 David 2023; Van der Wagen, Oerlemans & Weulen Kranenbarg 2020b.
50 Zie ook Oerlemans 2017a.
51 Kort & Spithoven 2021.
52 https://www.nrc.nl/nieuws/2022/11/16/van-abusehosting-tot-tot-fuckservers-we-kennen-de-deals-en-de-namen-maar-ingrijpen-is-lastig (voor het laatst geraadpleegd op 3 januari 2023).
53 Resellers zijn klanten – vaak buitenlandse bedrijven – van Nederlandse hostingbedrijven die serverruimte 'onderhuren'. Klanten huren voor een maand of soms een dag serverruimte, betalen met virtuele valuta, voeren hun criminele activiteiten uit en verdwijnen dan weer.
54 Zie bijvoorbeeld: https://www.nrc.nl/nieuws/2022/11/16/van-abusehosting-tot-tot-fuckservers-we-kennen-de-deals-en-de-namen-maar-ingrijpen-is-lastig (voor het laatst geraadpleegd op 3 januari 2023).
55 Lees bijvoorbeeld: https://magazines.openbaarministerie.nl/opportuun/2022/03/esther-baars (voor het laatst geraadpleegd op 2 januari 2023).

zooi het internet op.[56] Het de-territoriale karakter van digitale criminaliteit in het algemeen en cybercriminaliteit in het bijzonder wijkt fundamenteel af van traditionele criminaliteit, die veel meer gebiedsgebonden is.

Het tweede kenmerk heeft betrekking op de mogelijkheden tot anonimiteit in de digitale of online wereld. Het internet stelt mensen in staat om in behoorlijke mate anoniem te blijven door onder andere pseudoniemen te gebruiken en gebruik te maken van allerlei middelen om hun identiteit te verhullen: Virtual Private Network (VPN)- en proxyservers, de Onion Router (Tor, zie hoofdstuk 7) of andere vormen van encryptie.[57] Plegers van digitale criminaliteit kunnen hun identiteit eenvoudig verhullen.[58] Identificatie bij digitale criminaliteit wijkt sterk af van identificatie bij traditionele criminaliteit.[59] De hulpmiddelen die er in de offline wereld zijn om personen te identificeren, zijn niet bruikbaar in de digitale wereld.[60] Door het internationale karakter van digitale criminaliteit – het gaat dan in het bijzonder om cybercriminaliteit – wordt identificatie verder bemoeilijkt.

Het derde kenmerk is het schaalniveau: digitale criminaliteit is veel meer schaalbaar dan traditionele criminaliteit. Met heel weinig inspanningen kunnen door één of enkele daders duizenden of miljoenen slachtoffers tegelijkertijd worden gemaakt. 'Crime scales exponentially', aldus Marc Goodman.[61] Digitale criminelen maken geregeld gebruik van het *minimis principe*:[62] heel veel mensen een klein beetje treffen. De schade per slachtoffer is soms zo klein dat slachtoffers minder noodzaak voelen om aangifte te doen dan wel de stimulans om deze delicten te onderzoeken en vervolgen aanzienlijk afneemt. De vraag is ook of deze gevallen moet worden beschouwd als één delict of als meerdere delicten.[63] Bij een woninginbreker die in dezelfde nacht bij verschillende huizen inbreekt, is een dergelijke vraag niet aan de orde. Het zijn verschillende delicten.

Het vierde kenmerk gaat over de rol die technologie speelt in de uitvoering van delicten. Voor het plegen van digitale criminaliteit is in toenemende mate allerlei software beschikbaar: *cybercrime-as-a-service*.[64] Er is software voor onder andere pishing, spam, DDoS-aanvallen en ransomware.[65] Deze 'crimeware' wordt ontwikkeld door

56 https://www.nrc.nl/nieuws/2022/11/16/van-abusehosting-tot-tot-fuckservers-we-kennen-de-deals-en-de-namen-maar-ingrijpen-is-lastig (voor het laatst geraadpleegd op 3 januari 2023).
57 David 2023; Oerlemans 2017a; Van der Wagen, Oerlemans & Weulen Kranenbarg 2020b.
58 Oerlemans 2017a.
59 Oerlemans 2017a; Stol 2020.
60 Hierbij komt dat de gebruiker van een apparaat niet per definitie de pleger van het delict is. Een crimineel kan een computer van iemand overnemen en daarmee bijvoorbeeld een cyberaanval uitvoeren (zie ook Schermer, 2022).
61 Goodman 2015: 219.
62 Van der Wagen, Oerlemans & Weulen Kranenbarg 2020b.
63 Zie ook Caneppele & Aebi 2017.
64 Van der Voort & Warnaars 2020.
65 Zie ook Europol 2023b.

criminele bedrijven die onder andere opereren op het darkweb en veel gemeen hebben met een regulier softwarebedrijf. Ze bieden standaardsoftware aan, maar zijn ook bereid en in staat om maatwerksoftware te maken, bijvoorbeeld voor criminele organisaties. Deze 'crimeware' bedrijven krijgen feedback van klanten over bugs, brengen updates uit, hebben een helpdesk en vragen klanten naar suggesties voor nieuwe functionaliteiten. Goodman vat samen: '… modern crime has become reduced and distilled to a software program that anybody can run at tremendous profit.'[66] Het plegen van digitale criminaliteit wordt hierdoor eenvoudiger en laagdrempeliger, ook waar het gaat om lucratieve vormen van cybercriminaliteit (waaronder ransomware).[67] De geautomatiseerde uitvoering van digitale criminaliteit draagt ook bij aan het voorgaande kenmerk: het schaalniveau.

Het vijfde en laatste kenmerk is de private context waarin digitale criminaliteit wordt gepleegd. Deze formulering heeft twee betekenissen. De eerste betekenis vloeit voort uit wat eerder is behandeld: de ontwikkeling van het internet is in belangrijke mate buiten het politieke domein tot stand gekomen. Hoewel de protocollen en standaarden van het internet kunnen worden beschouwd als een publiek goed,[68] zijn gebruikers vooral afhankelijk van de bedrijven die de kabels, servers, verbindingen, platformen, et cetera in hun bezit hebben. Digitale criminaliteit speelt zich in belangrijke mate af in het private domein. Dit heeft onder andere als gevolg dat de politie – veel meer dan bij traditionele criminaliteit – moet samenwerken met private partijen. De tweede betekenis van privaat heeft te maken met de plaats waar delicten worden gepleegd: daders hoeven de deur niet of nauwelijks uit. Het gedrag van de dader is niet of nauwelijks zichtbaar in het publieke domein.[69] Dit is een wezenlijk verschil met veel traditionele criminaliteit die plaatsvindt in het publieke domein met zichtbare handelingen van daders die tevens meer 'reallife' consequenties van hun handelen ondervinden.

Het gegeven dat digitale criminaliteit geen 'oude wijn in nieuwe zakken' is, maakt dat digitale criminaliteit maar moeizaam kan worden aangepakt vanuit het 'veiligheidsprogramma' of -paradigma – het geheel van uitgangspunten (bijvoorbeeld criminologische theorieën),[70] spelers, middelen en spelregels – dat de traditionele criminaliteit heeft teruggedrongen.[71] Dit heeft als gevolg dat de aanpak van digitale criminaliteit voor zowel de politie als anderen een stevige opgave is.

66 Goodman 2015: 219.
67 Zie ook de NCTV 2023 over de professionalisering en commercialisering van 'criminele tools en diensten'.
68 Zie hiervoor de WRR 2015.
69 Weulen Kranenbarg 2018.
70 Weulen Kranenbarg 2018; Van der Wagen 2018.
71 Zie ook Goodman 2015.

7 Technologie en georganiseerde criminaliteit

Netwerken die zich bezighouden met georganiseerde criminaliteit worden beschouwd als een *early adopter* van technologie.[1] Dit wil zeggen dat zij nieuwe technologische mogelijkheden – zo snel mogelijk – gebruiken voor de uitvoering van criminele processen. Dit hoofdstuk gaat in op de invloed van technologie op de georganiseerde criminaliteit. Eerst komen de toenemende zorgen over de georganiseerde criminaliteit in Nederland aan bod en daarna staat de invloed van technologie centraal.

Toenemende zorgen over de georganiseerde criminaliteit

Er is sprake van georganiseerde criminaliteit als groepen, die primair gericht zijn op illegaal gewin, systematisch misdaden plegen met ernstige gevolgen voor de samenleving, en in staat zijn om deze misdaden op betrekkelijk effectieve wijze af te schermen.[2] In Nederland zijn sinds de daling van de geregistreerde criminaliteit is ingezet – en dan vooral de laatste vijf tot tien jaar – de zorgen over de aard en omvang van de georganiseerde criminaliteit toegenomen. Deze zorgen hebben vooral te maken met de ondermijnende gevolgen voor samenleving, economie en rechtsstaat.[3] Hoe omvangrijk de georganiseerde criminaliteit in Nederland is, weten we niet en ook van de gevolgen hebben we een onvolledig beeld.[4] Duidelijk is in ieder geval wel dat zich in de afgelopen decennia grote criminele netwerken op lokaal, regionaal, nationaal en internationaal niveau hebben ontwikkeld, die zich bezighouden met georganiseerde criminaliteit in het algemeen en met drugscriminaliteit in het bijzonder.[5] Nederland vervult al decennialang een prominente rol in de internationale drugshandel als bronland van cannabis en synthetische drugs en als doorvoerland van vooral cocaïne.[6] Georganiseerde criminaliteit is dan ook vooral – maar zeker niet alleen – drugscriminaliteit.[7]

Het is aannemelijk dat de rol van Nederland in de internationale drugshandel in de afgelopen jaren belangrijker is geworden, in het bijzonder voor wat betreft de rol in de

1 Bastrup-Birk et al. 2023; Europol 2021a; Goodman 2015.
2 Enquêtecommissie opsporingsmethoden 1996.
3 Peters 2018.
4 Zie ook Fijnaut 2021.
5 Spapens & Van de Mheen 2022; Werdmölder 2022.
6 Noordanus 2020.
7 Fijnaut (2021) formuleert het anders en stelt dat de illegale drugsindustrie het centrale probleem is in de zware, georganiseerde criminaliteit in Nederland.

internationale cocaïnesmokkel.[8] Het vele drugsgeld[9] dringt door tot vrijwel alle sectoren van de bovenwereld. Vermenging van onder- en bovenwereld is dan ook volop gaande, onder andere in havens,[10] de sierteelt,[11] de visserij[12] en het goederen(weg) vervoer.[13] Ook valt op dat het geweld excessiever is geworden.[14] De liquidaties die zijn gerelateerd aan de georganiseerde drugscriminaliteit hebben een grover en slordiger karakter gekregen[15] én zijn meer gericht op (publieke) personen uit de bovenwereld.[16] De moorden op Derk Wiersum en Peter R. de Vries – maar ook de vele bedreigingen – maken duidelijk dat de georganiseerde criminaliteit in toenemende mate de rechtsstaat is gaan aantasten. Dat is een verschil met tien of twintig jaar geleden.[17] Er zijn tevens toenemende zorgen over de betrokkenheid van jongeren in de georganiseerde drugscriminaliteit.[18] Die betrokkenheid is een gevolg van rekrutering[19] of eigen initiatief en kan het karakter hebben van criminele uitbuiting.[20] Een (klein) deel van deze 'jonge aanwas' groeit door van de onderlaag naar de midden- en bovenlaag[21] van de georganiseerde misdaad.[22] Volgens het Openbaar Ministerie (OM) in Nederland wordt die stap steeds sneller gemaakt.[23]

Nieuwe technologie, nieuwe mogelijkheden

Op basis van het voorgaande lijkt er voldoende aanleiding om te veronderstellen dat de georganiseerde criminaliteit in Nederland erger is geworden.[24] De georganiseerde (drugs)criminaliteit is voor (onder andere) de politie – nu en in de toekomst – een 'serieuze opponent'.[25] Deze opponent benut nieuwe technologieën voor de uitvoering van criminele processen.

8 McDermott et al. 2021; Fijnaut 2021; Werdmölder 2022.
9 Tops & Tromp (2022) schatten het vermogen van de Nederlandse drugsindustrie op zo'n 40 miljard euro.
10 Zie bijvoorbeeld https://www.nrc.nl/nieuws/2021/04/25/criminelen-infiltreren-in-rederijen (voor het laatst geraadpleegd op 27 december 2021).
11 Van der Torre et al. 2021.
12 Mehlbaum et al. 2021.
13 Bervoets et al. 2021.
14 Europol 2021b; Fijnaut 2021; Werdmölder 2022.
15 Van Gestel & Verhoeven 2017.
16 Leistra 2020.
17 Fijnaut 2021; 2023.
18 Ferwerda et al. 2021; SMV 2022; Weijers, Ferwerda & Roks 2021.
19 Zie bijvoorbeeld https://www.parool.nl/amsterdam/de-onderwereld-werft-jongeren-als-kindsoldaten-ze-zijn-voor-de-bazen-inwisselbaar (voor het laatst geraadpleegd op 2 januari 2023).
20 Leito, Van Bemmel & Noteboom 2021.
21 Zo is de 'mocromaffia' voortgekomen uit een jeugdgroep die aan het begin van deze eeuw actief was in de Diamantbuurt in De Pijp in Amsterdam en is Ridouan Taghi begonnen als onderdeel van de jeugdgroep 'Bad Boys' in de regio Utrecht. Dergelijke jeugdgroepen zijn de 'kraamkamer' van de georganiseerde misdaad (zie Ferwerda et al. 2021).
22 Kruisbergen, Roks & Kleemans 2019.; Weijers, Ferwerda & Roks 2021.
23 Van Liempt 2022.
24 Zie ook Fijnaut 2021.
25 Meershoek 2018.

'Information technology represents a powerful and effective tool for criminals, for supporting the creation of new criminal scenarios, simplifying the execution of specific illegal activities, and reducing the risk of detection.'[26]

In het vervolg van dit hoofdstuk wordt op hoofdlijnen uitgewerkt op welke wijze technologie de georganiseerde criminaliteit beïnvloedt. Het gaat hierbij in de eerste plaats om de aard van de criminaliteit die criminele netwerken plegen. Kenmerkend voor deze netwerken dat zij in de regel van meerdere criminele markten thuis zijn.[27] Zij zijn, tot op zekere hoogte, in staat om flexibel te opereren en passen zich aan op kansen en bedreigingen in hun omgeving.[28] Het domein van digitale criminaliteit biedt criminele netwerken nieuwe mogelijkheden (zie ook het vorige hoofdstuk).[29] Digitale criminaliteit is een nieuw verdienmodel,[30] naast de traditionele criminaliteit die zij in meer of mindere mate blijven plegen.[31] Er is in die gevallen een hybride situatie ontstaan waarin traditionele criminaliteit en digitale criminaliteit met elkaar worden gecombineerd.[32] De coronapandemie heeft voor een versnelling gezorgd in de uitbreiding van de activiteiten van criminele netwerken naar digitale criminaliteit.[33]

De invloed van technologie op de georganiseerde criminaliteit heeft daarnaast betrekking op de wijze waarop criminaliteit wordt gepleegd. Technologie biedt criminele netwerken nieuwe mogelijkheden op het gebied van samenwerking, uitvoering van logistieke aspecten van het criminele proces en de omgang met de geldstromen.[34] Europol merkt hierover het volgende op:

'The use of technology is a key feature of serious and organised crime […] Criminals exploit encrypted communications to network among each other, use social media and instant messaging services to reach a larger audience to advertise illegal goods or to spread disinformation. The online environment and online trade provide criminals access to expertise and sophisticated tools enabling criminal activities.'[35]

Een eerste aspect dat in dit kader aandacht verdient, is het ontstaan van online markten voor illegale goederen en diensten op het darkweb: *dark markets*.[36] Een dark market is een online forum waarop goederen en diensten worden uitgewisseld tussen partijen

26 Tundis & Mühlhäuser 2020: 60.
27 Europol 2021a.
28 Boutellier, Hermans & Van de Plas 2019; Europol 2021a; Tops & Tromp 2020.
29 Antonopoulos & Papanicolaou 2018.
30 Zeker niet alle criminele structuren zijn zich met digitale criminaliteit gaan bezighouden. Het zijn vooral de criminele structuren die zich bezighouden met georganiseerde vormen van vermogenscriminaliteit die in de digitale criminaliteit zijn 'gestapt' (zie Kruisbergen et al. 2018; Leukfeldt & Roks, 2021).
31 Leukfeldt & Holt 2022.
32 Roks, Leukfeldt & Densley 2020.
33 Europol 2021a: 94.
34 Bastrup-Birk et al. 2023; Kruisbergen et al. 2018.
35 Europol 2021a: 11.
36 Bird et al. 2020; Kruisbergen et al. 2018; Oerlemans & Wegberg 2019; Tundis & Mühlhäuser 2020.

die gebruikmaken van digitale encryptie om hun identiteit te verbergen.[37] Deze markten faciliteren de handel in onder andere drugs, wapens en kinderporno en heffen – mede afhankelijk van de goederen en diensten die worden verhandeld – beperkingen in tijd en ruimte voor een groot deel op. De markt van kopers is hierdoor internationaler geworden.[38] Dit geldt ook voor illegale producten die fysiek moeten worden geleverd, zoals drugs. In 2020 lieten politie en justitie via het *NRC* weten dat zij klachten kregen van opsporingsdiensten uit het buitenland die werden 'overspoeld' met drugspakketten uit Nederland.[39] Dit is een indicatie van het stevige aandeel dat onlinedrugshandelaren uit Nederland hebben op de internationale dark markets.[40] De coronapandemie heeft ervoor gezorgd dat de handel op het darkweb – in ieder geval voor wat betreft drugs – verder tot bloei is gekomen.[41] Ondanks dat er regelmatig grote dark markets door opsporingsdiensten worden 'verstoord' en 'gesloten'[42], blijkt dat beheerders, verkopers en kopers over adaptief vermogen beschikken: er zijn in die gevallen meer, kleinere markten ontstaan en de verwachting is dat deze trend zich door gaat zetten.[43] Daarnaast zijn Telegram Messenger en andere apps voor beveiligde berichtenuitwisseling in toenemende mate een alternatief voor het gebruik van dark markets.[44] Vraag en aanbod op het gebied van onder andere drugs, digitale criminaliteit en excessief geweld komen hier bij elkaar.

Met de opkomst van het darkweb zijn er ook online criminele ontmoetingsplaatsen ontstaan die de samenwerking tussen en binnen criminele netwerken faciliteren.[45] Deze *dark forums* heffen de traditionele beperkingen van sociale netwerken op.[46] De werking van deze online ontmoetingsplaatsen is vergelijkbaar met die van de traditionele ontmoetingsplaatsen: zodra je binnen bent, kun je personen ontmoeten die kunnen bijdragen aan het uitvoeren van criminele processen of aan nieuwe afzetmarkten. Het is niet veel anders dan een bar vol criminelen – zoals voorheen de Partyking in

37 Het worden om die reden ook wel cryptomarkten genoemd (zie bijvoorbeeld Van Valkenhoef, De Groes & Tops, 2022), maar deze term heeft niet mijn voorkeur vanwege mogelijke verwarring met markten voor cryptovaluta. Overigens moet wel worden opgemerkt dat de handel op dark markets veelal wordt betaald met crypto- of virtuele valuta.

38 Bastrup-Brik et al. 2023; Kassab & Rosen 2019.

39 https://www.nrc.nl/nieuws/2020/06/29/nederland-internationaal-onder-vuur-om-drugshandel-per-post (voor het laatst geraadpleegd op 28 december 2021).

40 Van Valkenhoef, De Groes & Tops 2022; zie ook Oerlemans & Wegberg 2019.

41 Zie https://www.vice.com/en/article/dyz3v7/online-drug-markets-are-entering-a-golden-age (voor het laatst geraadpleegd op 5 december 2021). Zie ook https://www.nu.nl/binnenland/6173975/douane-onderschepte-in-2021-fors-meer-drugspakketten-topje-van-de-ijsberg.html (voor het laatst geraadpleegd op 28 december 2021). Zie ook: Van Valkenhoef, De Groes & Tops 2022.

42 Dit betreft onder andere de Hansa-operatie die is uitgevoerd door het Team High Tech Crime (THTC) van de landelijke eenheid waarbij de online drugsmarktplaats 'Hansa' gedurende een maand werd overgenomen (zie hoofdstuk 18).

43 Bird et al. 2020; Van Valkenhoef, De Groes & Tops 2022.

44 Zie bijvoorbeeld Moyle et al. 2019.

45 Zie Europol (2023) over de rol van deze 'underground communities' in cybercriminaliteit. Hierbij moet worden benadrukt dat deze online gemeenschappen in allerlei vormen van georganiseerde criminaliteit een rol spelen.

46 Kruisbergen et al. 2018.

Brabant[47] – behalve dat je de deur niet uit hoeft en de toegang laagdrempeliger lijkt te zijn.[48] Er zijn op fora ook rating- en reviewsystemen, zodat je een inschatting kunt maken van onder andere de vaardigheden en betrouwbaarheid van degene met wie je in zee gaat.[49] Deze online netwerken en contacten fungeren naast offline netwerken, net zoals in het leven van 'gewone' burgers (zie hoofdstuk 2).

De invloed van technologie op de samenwerking binnen en tussen criminele netwerken reikt verder dan online ontmoetingsplaatsen. Men moet, over landsgrenzen heen, met elkaar communiceren en opereert onder heimelijke condities.[50] Afgeschermde communicatie is daarom essentieel. Criminele netwerken zijn voor afgeschermde communicatie in belangrijke mate afhankelijk van technologie.[51] Hierbij kan worden gedacht aan technische middelen om afluisteren tegen de te gaan, bulletproof hosting – dit zijn afgeschermde datacenters – en in het bijzonder aan versleutelde communicatie. Via geëncrypte telefoons en een gesloten netwerk wordt geprobeerd om het risico op interceptie door opsporingsinstanties te minimaliseren.[52] Het risico op interceptie blijft niettemin aanwezig, getuige de interceptie in het kader van onder andere Ironchat, Ennetcom, Encrochat en Sky Ecc (zie hoofdstuk 12). Maar ook hiervoor geldt: de georganiseerde criminaliteit past zich aan op diens bestrijders.[53] Zo nemen de zorgen over het gebruik van 'stenografie' toe.[54] Boodschappen worden dan verstopt, bijvoorbeeld door deze op te nemen in de kleurwaardes van een digitale foto.

Criminele netwerken benutten – tot slot – de opkomst van virtuele valuta, ook wel cryptovaluta genoemd, in de omgang met geldstromen. Virtuele valuta kunnen worden beschouwd als een facilitator van criminele verdienmodellen en zijn een vitaal onderdeel geworden van verschillende criminele bedrijfsprocessen.[55] Virtuele valuta worden vooral gebruikt voor 1) betalingen voor illegale goederen & diensten op het darkweb, 2) betalingen voor cyberaanvallen (in het bijzonder ransomware), en 3) witwassen van criminele verdiensten.[56] De blockchaintechnologie maakt het mogelijk om

47 Zie hiervoor Tops & Tromp 2017.
48 Leukfeldt, Kleemans & Stol 2017.
49 Ook voor dark forums geldt dat apps voor beveiligde berichtenuitwisseling (waaronder Telegram Messenger) in toenemende mate als alternatief of aanvulling worden gebruikt.
50 Duijn 2016.
51 Kassab & Rosen 2019; Kruisbergen, Roks & Kleemans 2019.
52 Ik beperk me hier tot versleutelde communicatie tussen personen in de boven- en middenlaag van criminele structureren. In de detailhandel vindt communicatie ook voor een belangrijk deel plaats via berichtenservices. Vooral de eerder aangehaalde berichtendienst Telegram Messenger wint aan populariteit (zie Van Valkenhoef et al., 2022). Telegram-gebruikers kunnen versleutelde berichten versturen en berichten kunnen zichzelf vernietigen. Privéberichten zijn vervolgens de opmaat naar de daadwerkelijke verkoop (zie Roks & Hendriksen, 2021). Sociale media spelen daarnaast een belangrijke rol bij het rekruteren van jongeren ten behoeve van de drugshandel (zie bijvoorbeeld Adjiembaks, Boer & Oude Lansink 2022).
53 Zie ook Jansen et al. 2023.
54 https://www.forensischinstituut.nl/actueel/nieuws/2022/07/26/we-moeten-alert-zijn-op-het-herkennen-van-verborgen-berichten-van-verdachten (voor het laatst geraadpleegd op 23 oktober 2022).
55 Greenberg 2022; Schrama et al.2022.
56 Silfversten et al. 2020.

op internationale schaal online, relatief anonieme[57] transacties uit te voeren zonder betrokkenheid van banken. Het gebruik van virtuele valuta in criminele processen is weliswaar in opkomst, maar aangenomen wordt dat dit gebruik nog steeds beperkt is.[58] Dit heeft mogelijk te maken met de nadelen van het gebruik van virtuele valuta in criminele processen.[59]

Samenvattend: als *early adopters* hebben criminelen die zich bezighouden met georganiseerde criminaliteit de mogelijkheden van technologie benut voor hun criminele praktijken.[60] Dit heeft, net als in legale markten, geleid tot vernieuwing in criminele markten en criminele samenwerking.[61] Ook in de komende jaren zullen zij de mogelijkheden van opkomende technologieën benutten om de politie en andere partijen voor te blijven in het kat-en-muisspel dat zo kenmerkend is voor de bestrijding van de georganiseerde criminaliteit.

57 De mate van anonimiteit verschilt per cryptovaluta en daarmee samenhangende blockchain. In principe zijn en blijven alle transacties zichtbaar op de blockchain en zijn deze dus traceerbaar. Het adres (de 'wallet') is geanonimiseerd. Er zijn ook zogenaamde 'privacy coins', zoals Monero, Dash en Zcash (zie Europol, 2021c). Bij het gebruik van deze coins zijn de verzendende en ontvangende adressen afgeschermd.

58 Europol 2021c; Schrama et al. 2022.

59 Deze nadelen houden onder andere verband met de traceerbaarheid van transacties, volatiliteit van virtuele valuta – de waarde kan ineens flink dalen – en het risico op het hacken van het adres c.q. de digitale portemonnee. Om die reden wordt – zeker in het deel van het proces waarin transacties met eindgebruikers plaatsvinden – gebruikgemaakt van alternatieve (virtuele) betaalwijzen, zoals prepaid debit en creditcards (zie Schrama et al., 2022).

60 Europol 2021a; Goodman 2015.

61 Bird et al. 2020.

8 Digitalisering en maatschappelijk ongenoegen

In hoofdstuk 2 is beschreven hoe de ontwikkeling van het internet in het algemeen en sociale media in het bijzonder hebben geleid tot het ontstaan van een digitale nevenwereld die is verweven met de fysieke wereld. Beide vormen een laag in de (sociale) realiteit die we ervaren. Hierdoor zijn sociale media in verschillende opzichten een belangrijke rol in onze samenleving gaan spelen. Sociale media kunnen bijdragen aan verbinding, maar ook aan verdeling in de samenleving. In dit hoofdstuk staat de rol van sociale media in het verdelen van de samenleving centraal.

Sociale media en identiteitspolitiek

De eerder aangehaalde Manuel Castells schreef in aanloop naar het huidige millennium een trilogie over het informatietijdperk. In het tweede deel hiervan – *Power of identity* – voorspelde hij dat het leven in een netwerksamenleving tot nieuwe identiteitsvorming zou gaan leiden rondom religie, etniciteit, nationaliteit en thema's als milieu en seksuele identiteit.[1] In het afgelopen decennium is steeds duidelijker geworden dat er in onze samenleving inderdaad allerlei nieuwe identiteitsvorming heeft plaatsgevonden dan wel dat bestaande identiteiten zijn versterkt. In een ver-netwerkte wereld biedt identiteit herkenning en gemeenschappelijkheid, zo stelt Hans Boutellier.[2] Deze herkenning wordt in toenemende mate gevonden in boosheid of *ressentiment*[3] onder burgers over de omstandigheden in de samenleving na drie decennia (neo[4])liberaal beleid.[5] Deze boosheid vloeit vooral voort uit het gevoel van burgers dat hun waardigheid wordt geschonden, gekleineerd of anderszins wordt miskend.[6] Dit doet hen terugvallen op de verbondenheid van de eigen groep.[7] Met die groep

1 Castells 1997.
2 Boutellier 2021.
3 Dit begrip wordt ontleend aan het werk van Nietzsche en verwijst naar een (geestelijke) toestand in mensen die zich machteloos voelen en wrok of boosheid ontwikkelen ten opzichte van degenen die in hun ogen hun identiteit en waardigheid niet of onvoldoende onderkennen (zie o.a. Mishra, 2017).
4 Met neoliberaal wordt in de regel vooral gewezen op een kleine, 'terugtredende' overheid die ruim baan geeft aan de markt en aan vrij verkeer van handel en kapitaal.
5 Zie voor uitgebreide analyses: Boutellier 2021; Van den Brink 2020; Fukuyama 2019; Guilluy 2019; Heijne 2019; Sadin 2021.
6 Boutellier 2021.
7 Heijne 2019.

wordt 'gestreden' om erkenning van de eigen identiteit en de daarmee samenhangende belangen. Deze strijd wordt *identiteitspolitiek* genoemd.[8]

De opkomst van het internet in het algemeen en sociale media in het bijzonder hebben een belangrijke rol gespeeld in het ressentiment en de daarmee samenhangende identiteitspolitiek.[9] In *Het tijdperk van de Ik-tiran* van Éric Sadin wordt de invloed van sociale media op de identiteitspolitiek en daaruit voortvloeiende afbrokkelende gemeenschappelijkheid uitvoerig beschreven.[10] Sadin laat zien hoezeer zowel de apparaten (iPhone) als de platformen en daarop functionerende algoritmen het individu als middelpunt nemen. Dit wordt ook wel uitgedrukt met 'just me and the internet'.

> *'… the architecture of online worlds – including the filter bubbles, recommender systems, user profiles and search algorithms – all work to enable users to seemingly create and live in a world (much more) on their own terms.'*[11]

De sociale netwerken spelen effectief in op ieders zucht naar erkenning en diepe behoefte zich te kunnen uiten.[12] Twitter, Facebook, Instagram, TikTok, YouTube en andere socialemediaplatformen zijn manieren om jouw identiteit te communiceren, te voeden en te onderzoeken. Ze stellen mensen in staat om tegenover bekenden of talloze wildvreemden te getuigen van momenten van echte of geveinsde blijdschap, of juist van ervaren problemen en verdriet, en tevens van eigen meningen, ontevredenheid en woede. Hier wordt naar hartenlust gebruik van gemaakt. Er is een industrie van *de uitingsdrang* ontstaan. Sociale zichtbaarheid is geen kwestie meer van daadwerkelijk eigen handelen en persoonlijke verdienste, maar wordt (ook) verkregen door verbale bevestiging en verspreiding van allerlei afbeeldingen en feiten die tot gevoelens van erkenning moeten leiden. Die erkenning wordt gevonden in gemeenschappen van gelijkgestemden en bij informatie die het individu bevestigt in diens eigen gelijk.

> *'Deze digitale "aanspreking tot subject" verschijnt op een geraffineerde manier als zelfgekozen. Maar ze is het resultaat van een proces dat we niet echt kunnen controleren. De ogenschijnlijke vrijheid in de bepaling van mijn route in de digitale netwerken, blijkt de facto gemanipuleerd door logaritmische navigatie. Ik zou in dat verband*

8 Fukuyama (2019) wijst erop dat deze identiteitspolitiek ook zichtbaar is in de manier waarop de politiek is georganiseerd. De oorspronkelijke betekenis van links en rechts heeft aan relevantie verloren. De politiek is meer georganiseerd op basis van identiteit. Op links is de nadruk minder komen te liggen op algemene economische gelijkheid en is men zich meer gaan richten op het begunstigen van de belangen van allerlei gemarginaliseerde groepen, zoals minderheden, vluchtelingen en lhtbi+'ers. Op rechts is er meer nadruk komen te liggen op patriottisme: het beschermen van de nationale identiteit, die dikwijls wordt verbonden aan ras, etniciteit of godsdienst.

9 Zie hiervoor onder andere Boutellier 2021; Beugelsdijk 2021; Fukuyama 2019 en 2021; Sadin 2021.

10 Sadin 2021.

11 Cocking & Van den Hoven 2018: 148.

12 Beugelsdijk 2021; Sadin 2021.

willen spreken van de "algoritmische opsluiting" van de eigen identiteit. We kunnen er formeel wel uitstappen, maar dat is niet gemakkelijk als je in feite bent ingesponnen.'[13]

De algoritmische opsluiting van de eigen identiteit is een gevolg van het gegeven dat we steeds meer online zijn gaan leven. We besteden de analyse van de wereld meer en meer uit aan machines en nu zijn we langzamerhand afhankelijk van deze machines voor ons begrip van de wereld en zelfs voor begrip van onszelf, aldus Maxim Februari.[14] De algoritmische opsluiting van de eigen identiteit resulteert in een *bubbel*: je leeft dan in een kring met mensen die dezelfde opvattingen hebben en komt informatie tegen die in lijn is met deze opvattingen.[15] Na verloop van tijd is het nog lastig om je voor te stellen dat er anderen zijn die de wereld totaal anders zien en ervaren.[16] Dit geldt dus ook voor die anderen. Gemeenschappen worden hierdoor niet meer begrensd door fysieke barrières, maar door het geloof in een gemeenschappelijk identiteit.[17] Dit is volgens Sadin de essentie van het tijdperk van de 'Ik-tiran': er ontstaat een overvloed aan ongebonden (groepen) individuen die alleen nog maar zichzelf erkennen als normatief referentiepunt en bron van gezag. Het is ook om die reden dat Boutellier sociale netwerken als hypermorele media beschouwt: het individu is door en door moralistisch ten opzichte van andere posities.[18] Dit is vooral zichtbaar op Twitter dat fungeert als maatschappelijke uitlaatklep.[19] Maatschappelijke discussies lopen uit de hand, resulterend in een gepolariseerd debat waarin zenden belangrijker is geworden dan luisteren.[20]

De identiteitspolitiek wordt niet alleen verhevigd doordat sociale netwerken helpen om medestanders te vinden en informatie aanreiken die in jouw straatje past, maar ook door de desinformatie die wordt verspreid. Desinformatie is weliswaar van alle tijden,[21] maar sociale media hebben gezorgd voor een oneindige hoeveelheid kanalen om deze informatie te laten voortwoekeren. Met de opkomst van *deep fakes* – gemanipuleerde content die niet meer van echt te onderscheiden is – gaat desinformatie een nieuw tijdperk in (zie het volgende hoofdstuk).[22] De betrouwbaarheid van informatie komt onder grote druk te staan, omdat foto's, video's, geluidsopnamen, menselijke stemmen, geschreven tekst et cetera allemaal nep kunnen zijn.[23] Er zijn op het internet

13 Boutellier 2021: 62.
14 Februari 2023.
15 Zie ook Coeckelbergh 2022.
16 Luyendijk 2017.
17 Fukuyama 2019.
18 Boutellier 2021.
19 Miltenburg et al. 2022; Sadin 2021.
20 Zie Beugelsdijk 2021; Miltenburg et al. 2022.
21 Klerks 2020.
22 Zie ook Eysink Smeets 2022.
23 Schick 2020.

niet of nauwelijks poortwachters om de kwaliteit van informatie te bewaken.[24] Algoritmen hadden hier wellicht een rol in kunnen vervullen, maar omdat het realiseren van zo veel mogelijk kliks het doel is, krijgen gebruikers informatie voorgeschoteld die aansluit bij hun bestaande voorkeuren en overtuigingen.[25] Uit onderzoek komt naar voren dat dit zich het meest voordoet bij gebruikers met conservatieve opvattingen: zij zijn meer geïsoleerd van andere opvattingen en zien de meeste desinformatie.[26]

Toenemende maatschappelijke onrust

Kort samengevat: de hoop dat internet de democratie zou versterken, is ijdel gebleken.[27] Een democratie bestaat bij de gratie van voldoende mensen die elkaar niet als vijanden, maar als opponenten zien en *grosso modo* over dezelfde feiten discussiëren.[28] Identiteitspolitiek leidt in een samenleving echter tot vijanddenken: 'met jou praat ik niet'.[29] Burgers in Nederland zijn dan ook bezorgd over de manier van samenleven. Ongeveer driekwart van de burgers denkt dat de tegenstellingen in Nederland de komende jaren gaan toenemen.[30] Tegenstellingen kunnen onvoorspelbare en potentieel gevaarlijke vormen aannemen, aldus Boutellier.[31] Het gaat hierbij niet alleen om tegenstellingen tussen groepen burgers, maar ook om wantrouwen ten opzichte van de overheid of breder: de traditionele instituties.[32] Met betrekking tot de tweede randvoorwaarde – discussiëren over dezelfde feiten – kan worden geconstateerd dat desinformatie de mogelijkheid van een betrouwbare, gedeelde werkelijkheid ondermijnt.[33] Hierdoor wordt het moeilijker om in de samenleving consensus te bereiken over belangrijke kwesties. Het sociale weefsel wordt aangetast doordat burgers voortdurend met ongeordende informatie worden bestookt.[34] Kortom: er is veel voor te zeggen dat de democratische rechtsstaat onder druk is komen te staan.[35] Hierbij speelt mee dat de huidige, representatieve democratie moeite heeft om een antwoord te vinden op de

24 Hierbij moet worden opgemerkt dat poortwachters alleen effect kunnen hebben als deze ook worden vertrouwd. Zo hebben factcheck-initiatieven om desinformatie tegen te gaan alleen zin als de instituten die de feiten checken, worden vertrouwd. Het gaat niet zozeer om wat je gelooft, maar om wie je gelooft. Zie hiervoor: https://www.nrc.nl/nieuws/2022/04/11/hoe-nepnieuws-in-je-brein-blijft-hangen (voor het laatst geraadpleegd op 26 juli 2022).

25 Fukuyama 2019.

26 Zie https://www.volkskrant.nl/nieuws-achtergrond/mega-onderzoek-van-208-miljoen-facebook-accounts-in-amerika-brengt-politieke-polarisatie-in-beeld (voor het laatst geraadpleegd op 15 augustus 2023).

27 Fukuyama 2022.

28 Müller 2021.

29 https://www.volkskrant.nl/columns-opinie/met-jou-praat-ik-niet-hoe-het-vijanddenken-oprukt-in-nederland (voor het laatst geraadpleegd op 26 juli 2022).

30 Miltenburg et al. 2022.

31 Boutellier 2021.

32 Wantrouwen ten opzichte van de overheid heeft verschillende verschijningsvormen en gradaties. In een column maakt Bas Heijne (naar mijn mening) een relevant onderscheid tussen de hysterische burger die de overheid ziet als het kwaad en de ontevreden burger die zich niet gezien voelt en zich opwindt over falend bestuur. Zie https://www.nrc.nl/nieuws/2023/06/02/de-hysterische-onbeschoftheid-tegen-halsema-is-echt-een-andersoort-bezorgdheid-dan-de-opwinding-over-falend-bestuur (voor het laatst geraadpleegd op 10 juli 2023).

33 Rauch 2021.

34 Februari 2023.

35 Zie ook Arentze et al. 2023.

nieuwe manieren waarop groepen burgers zich met behulp van technologie organiseren en uiten.[36]

De politie heeft nu en in de komende jaren te maken met de gevolgen van een democratie onder druk. De boosheid onder burgers heeft zich gemanifesteerd als een nieuw veiligheidsvraagstuk: maatschappelijk ongenoegen of maatschappelijke onrust.[37] Spanningen tussen bevolkingsgroepen en verzet tegen de overheid zijn hier verschijningsvormen van, die meer concreet zichtbaar worden in onder andere allerlei vormen van *evil online* – waaronder doxing en bedreigingen – en (online aangejaagde) verstoringen van de openbare orde.[38] De Nederlandse samenleving is sinds enkele jaren in woelig vaarwater terechtgekomen. De coronapandemie is hiervoor niet zozeer dé oorzaak geweest, maar heeft vooral als een versneller van al langer bestaande ontwikkelingen gefungeerd.[39] Zo staat het anti-overheidsextremisme sinds de coronapandemie nadrukkelijk op het vizier van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).[40] Daarnaast moet worden opgemerkt dat geopolitieke spanningen – zoals de oorlog in Oekraïne – gepaard gaan met (onder andere) online beïnvloedingscampagnes. Dit kan in Nederland maatschappelijk ongenoegen verder aanwakkeren.[41]

Nieuwe bedreigingen en onzekerheden leiden onder andere door sociale media sneller tot hevigere maatschappelijke onrust. Vertrouwen in (beleid van) bestuur en politiek kan normaal gesproken tegenwicht aan onrust bieden, maar juist dat vertrouwen is afgenomen. We hebben te maken met een opeenstapeling van crises,[42] die onder andere leidt tot toenemende armoede onder de Nederlandse bevolking.[43] Volgens hoogleraar Jan Rotmans koerst Nederland af op een periode van langdurige sociale onrust.[44] Hier zal de politie haar handen vol aan hebben. Niet alleen in operationele zin, maar ook in termen van positiebepaling. De politie in Nederland beweegt zich tussen de rechtsstaat en haar burgers én tussen overheid en gemeenschap.[45] Wanneer er juist in die verhoudingen toenemende spanningen ontstaan, is positiebepaling een dilemma. In een democratische samenleving kan het morele gezag van de politie namelijk

36 Zie ook https://platformoverheid.nl/artikel/nieuwe-publieke-arena-vraagt-om-leiderschap (voor het laatst geraadpleegd op 26 juli 2022).
37 Zie ook de definiering van de NCTV: https://www.nctv.nl/onderwerpen/maatschappelijke-onrust .
38 Verstoringen van de openbare orde moeten nadrukkelijk worden onderscheiden van het uitoefenen van het demonstratierecht. In een 'woelige' samenleving is demonstreren een van de middelen om als groep een mening te laten horen (zie ook Amnesty International, 2023). Zie ook hoofdstuk 27.
39 Eysink Smeets 2022.
40 NCTV 2022b; zie ook Van Meeteren 2022.
41 Bekkers et al. 2023.
42 Zie voor een internationaal perspectief: Roubini 2022.
43 Zie hiervoor de ramingen van het Centraal Planbureau. Ik baseer me op die van augustus 2022. Zie https://www.cpb.nl/augustusraming-2022 (voor het laatst geraadpleegd op 23 augustus 2022).
44 Zie onder andere deze video: https://www.youtube.com/watch?v=1BYcN7XonE8 (voor het laatst geraadpleegd op 6 oktober 2022).
45 Boutellier 2020.

niet alleen zijn verankerd in de rechtsstaat, maar moet die ook door (groepen in) de samenleving worden geaccepteerd.

9 Opkomende technologieën, opkomende fenomenen

De opkomende technologieën die in dit boek zijn behandeld, zullen in dit decennium hun stempel drukken op de aard en omvang van de digitale criminaliteit in het algemeen en cybercriminaliteit in het bijzonder. In dit hoofdstuk staan opkomende fenomenen centraal. Ik ga achtereenvolgens in op opkomende technologieën als doel van criminaliteit, opkomende technologieën als middel bij criminaliteit (met specifiek aandacht voor *deepfakes*) en criminaliteit in de metaverse.

Opkomende technologieën als doel van criminaliteit
In de wetenschappelijke literatuur verschijnen steeds meer artikelen over de nieuwe gelegenheidsstructuur die het Internet of Things (IoT) plegers van criminaliteit gaat bieden.[1] Het IoT bestaat uit een toenemend aantal apparaten dat draadloos met het internet en elkaar is verbonden (zie hoofdstuk 3). De combinatie van steeds meer apparaten en hun onderlinge connectie zorgt voor kwetsbaarheid voor cybercriminaliteit.[2]

> *'Connecting more devices will mean greater vulnerability, partly because there are more points of attack, and partly because the complexity of interactions between resource-poor devices increases with the number and variety of those devices.'*[3]

In de afgelopen jaren is al zichtbaar geworden dat veel apparaten – zeker voor consumentengebruik[4] – onvoldoende beveiligd zijn.[5] De vele 'dingen' van het IoT bieden veel ingangen om IoT systemen aan te vallen met onder andere DDoS of ransomware.[6] Door de connectiviteit kan het uitvoeren van bijvoorbeeld DDoS-aanvallen op

1 Blythe & Johnson 2021; Ciancaglini et al. 2020; Tuptuk & Hailes 2019.
2 Tuptuk & Hailes 2019.
3 Idem: 302.
4 Blythe & Johnson 2021.
5 Oerlemans & Van der Wagen 2020.
6 De EU heeft minimumeisen gesteld waaraan op het internet aangesloten apparaten moeten voldoen. Apparaten die hier niet aan voldoen, worden vanaf medio 2024 binnen de EU verboden. https://www.rijksoverheid.nl/actueel/nieuws/2021/10/29/minimumeisen-aan-digitale-veiligheid-slimme-apparaten (voor het laatst geraadpleegd op 3 januari 2023). Deze regelgeving kan echter niet voorkomen dat er al honderdduizenden en misschien wel miljoenen apparaten in Nederland zijn waarvoor deze eisen niet hebben gegolden. In die apparaten worden regelmatig softwarelekken ontdekt. Zie https://nos.nl/artikel/2449517-onveilige-slimme-apparaten-straks-van-de-markt-geweerd-maar-risico-s-blijven (voor het laatst geraadpleegd op 3 januari 2023).

netwerken of het infecteren van apparaten in netwerken grote gevolgen hebben.[7] Deze gevolgen zijn onder andere afhankelijk van het type of doel van het IoT-systeem. In de vitale infrastructuur zijn de risico's groot. Er wordt in toenemende mate ransomware ontwikkeld die zich specifiek richt op het aanvallen van industriële controlesystemen (ICS) die worden gebruikt voor bijvoorbeeld de drinkwater- en energievoorziening.[8] Maar denk ook aan het grootschalig c.q. georganiseerd hacken van omvormers van zonnepanelen waarmee het stroomnet kan worden gesaboteerd.[9]

Als het IoT diens potentieel gaat waarmaken in onder andere huizen, steden, mobiliteit en gezondheidszorg, dan nemen ook in die domeinen de risico's toe.[10] Een relatief onschuldig voorbeeld kwam begin 2021 in de media: 'slimme seksspeeltjes' die kunnen worden overgenomen door hackers.[11] Maar zorgelijker is het hacken van medische apparaten, zoals insulinepompen en pacemakers,[12] of van autonome voertuigen, zoals zelfrijdende auto's en drones.[13] Moord kan op deze wijze nieuwe verschijningsvormen krijgen en hetzelfde geldt voor diefstal, chantage en stalking.[14]

> *'Naarmate technologie meer verweven raakt met het menselijk lichaam, ontstaan nog weer nieuwe mogelijkheden tot het plegen van criminaliteit met impact op dat lichaam. Het kan gaan om delicten die nu in de cybercrimestatistieken nog niet voorkomen, zoals moord (hacken pacemaker), mishandeling (hacken prothese), aanranding (hacken gheisha balls), maar natuurlijk ook het dreigen met dergelijk geweld tegen het lichaam.'*[15]

Naast IoT-systemen zullen ook (andere) AI-systemen in toenemende mate doelwit worden van criminaliteit.[16] Begin 2023 waarschuwde de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) voor het groeiende risico van aanvallen op AI-systemen, waaronder het bewerken van de input, backdoor-aanvallen om het algoritme aan te passen en het stelen van het model.[17]

7 Oerlemans & Van der Wagen 2020.
8 NCTV 2020; Tuptuk & Hailes 2019.
9 https://nos.nl/artikel/2477105-zonnepanelen-hacken-om-te-ontwrichten-goed-naar-kijken-nu-geen-paniek (voor het laatst geraadpleegd op 10 juli 2023).
10 Zie bijvoorbeeld Hodgers 2021 over smart homes. Zie ook https://www.nytimes.com/2023/02/17/realestate/smart-home-devices.html (voor het laatst geraadpleegd op 22 februari 2023).
11 https://www.nu.nl/tech/6121291/slimme-seksspeeltjes-konden-worden-overgenomen-door-hackers.html (voor het laatst geraadpleegd op 2 augustus 2021).
12 Zie ook Stol 2020.
13 Ciancaglini et al. 2020
14 Tuptuk & Hailes 2019.
15 Stol 2020: 20.
16 Zie ook Hayward & Maas 2021.
17 AIVD 2023.

Opkomende technologieën als middel voor criminaliteit
Opkomende technologieën kunnen niet alleen doelwit zijn van, maar ook middel zijn bij het plegen van (digitale) criminaliteit. AI speelt hierin een sleutelrol. Het gebruik van AI voor het plegen van digitale criminaliteit bevindt zich momenteel in een beginstadium, maar de verwachting is dat dit gebruik zal toenemen en wijdverspreid zal raken.[18] Dit heeft consequenties voor de aard en mogelijk ook voor de omvang van de digitale criminaliteit. Ik licht een aantal van deze consequenties toe.

Het gebruik van AI door criminelen leidt in de eerste plaats tot het optimaliseren van bestaande *modus operandi* voor het plegen van digitale delicten. Deze optimalisering is een uitvloeisel van een centraal kenmerk van AI: het leervermogen van systemen (zie hoofdstuk 5). Dit leervermogen zorgt ervoor dat delicten – zoals hacken, malware, ransomware en phishing – steeds geraffineerder kunnen worden gepleegd en beveiligingsmaatregelen beter kunnen worden omzeild.

AI maakt grootschalige, geraffineerde vormen van phishing mogelijk
Op dit moment is de dominante *modus operandi* in het kader van phishing als volgt: men benadert een grote groep mensen met een algemeen bericht. Het delict is gebaseerd op het gemak waarmee kan worden geschaald. Er hoeft maar een fractie van de potentiële slachtoffers op in te gaan om toch een behoorlijk bedrag te vergaren (zie hoofdstuk 6). AI maakt het echter mogelijk om op grote schaal berichten op maat te maken – dit wordt ook wel 'spear phishing' genoemd – om zo het succespercentage te vergroten. Hierbij kan de AI-software onder andere gebruikmaken van informatie van sociale media en/of de stijl van de 'betrouwbare partij', die als afzender van het bericht fungeert. 'Rather than sending uniform messages to all targets, likely to miss the mark in most cases, the messages could instead be tailored to prey on the specific vulnerabilities inferred for each individual, effectively automating the spear-phishing approach. Additionally, AI methods could use active learning to discover "what works", varying the details of messages to gather data on how to maximize responses.'[19] ChatGPT – zie hoofdstuk 5 – kan bijvoorbeeld onder andere worden gebruikt voor het maken van authentieke teksten, mits de gebruiker de juiste opdrachten (prompts) geeft en hiermee de ingebouwde beveiligingsmaatregelen van ChatGPT weet te omzeilen.[20] Er ontstaan daarnaast op maat gemaakte LLM's voor het plegen van allerlei vormen van online fraude, zoals FraudGPT[21] en WormGPT,[22]

18 Ciancaglini et al. 2020; Oerlemans & Van der Wagen 2020.
19 Caldwell et al. 2020: 7.
20 Zie onder andere Europol 2023a; NCTV 2023.
21 https://thehackernews.com/2023/07/new-ai-tool-fraudgpt-emerges-tailored.html (voor het laatst geraadpleegd op 31 juli 2023).
22 https://www.ccinfo.nl/van-a-tot-z/ai/nieuws-ai/1400786_de-opkomst-van-wormgpt-een-nieuwe-dreiging-in-de-wereld-van-cybercriminaliteit (voor het laatst geraadpleegd op 31 juli 2023).

> die worden aangeboden op het darkweb en in besloten groepen van met name Telegram.

Een tweede consequentie van het gebruik van AI door criminelen heeft te maken met het gemak waarmee digitale criminaliteit kan worden gepleegd en geoptimaliseerd. Zo kan de huidige versie van ChatGPT al worden gebruikt om code voor malware te schrijven en dit zal zich naar verwachting verder ontwikkelen.[23] In meer algemene zin zal het gebruik van AI leiden tot een volgende stap in de automatisering van criminaliteit.[24] De 'cybercrime as a service' – software waarmee je zonder (veel) ICT-expertise digitale criminaliteit kunt plegen (zie hoofdstuk 6) – wordt door AI steeds geavanceerder.[25] De machines nemen niet meer alleen taken over, maar nemen zelfstandig beslissingen over uit te voeren acties én leren van deze acties. Zo wordt het steeds gemakkelijker om digitale criminaliteit op professionele wijze en omvangrijke schaal te plegen.

> *'The Crime-as-a-Service (CaaS) business model, which allows non-technologically savvy criminals to procure technical tools and services in the digital underground that allow them to extend their attack capacity and sophistication, further increases the potential for new technologies such as AI to be abused by criminals and become a driver of crime.'*[26]

Digitale criminaliteit gaat als gevolg van AI een punt bereiken waarop een deel van de delicten vrijwel volledig kan worden geautomatiseerd en er niet of nauwelijks menselijke interventies hoeven plaats te vinden (*crime by AI*). Dit brengt met zich mee dat technologie in toenemende mate als 'mededader' van digitale criminaliteit kan worden beschouwd,[27] zoals al het geval is bij het gebruik van onder andere botnets.[28] Dit wil zeggen dat er *actorschap* aan technologie kan worden toegekend.[29] De mens is niet meer de (enige) centrale kracht achter (de uitvoering van) criminele activiteiten. Dit impliceert niet dat de verantwoordelijkheid kan of moet worden afgeschoven op technologie in plaats van de mens, maar het zorgt er wel voor dat bijvoorbeeld het vaststellen van causaliteit bij geavanceerde vormen van digitale criminaliteit lastig kan zijn, omdat menselijke handelingen zijn verdwenen.

---

23 Europol 2023a. Wederom geldt: de gebruiker moet beveiligingsmaatregelen omzeilen, bijvoorbeeld door de opdracht in stappen op te delen.
24 Hayward & Maas 2021; Oerlemans & Van der Wagen 2020.
25 Caldwell et al. 2020; NCTV 2023.
26 Ciancaglini et al. 2020.
27 Van der Wagen 2018.
28 Een botnet is een verzameling van bots. Een bot is een computerprogramma dat autonoom taken kan uitvoeren. Een botnet ontstaat als de aanvallers of daders erin slagen om bots te installeren op apparaten die zijn verbonden met het internet. De botnets kunnen vervolgens worden gebruikt om criminele activiteiten uit te voeren, zoals een DDoS-aanval of het verspreiden van malware. Een botnet wordt dus niet alleen aangestuurd door de mens, maar ook door de machine. Dit wordt ook wel een hybride crimineel-actor netwerk genoemd. Zie hiervoor het proefschrift van Wytske van der Wagen (2018).
29 Zie ook Hayward & Maas 2021.

Een derde en laatste aspect dat valt onder het gebruik van AI voor het plegen van delicten heeft betrekking op *deep fakes*. Dit fenomeen is in het vorige hoofdstuk al benoemd. Vanwege de (verwachte) relevantie van dit fenomeen, zoom ik er op in.

Inzoomen: deepfake

Een deepfake is beeld, geluid of ander materiaal dat geheel of gedeeltelijk is gefabriceerd óf bestaand beeld, geluid of ander materiaal dat is gemanipuleerd met behulp van geavanceerde technische hulpmiddelen en dat niet of nauwelijks van echt te onderscheiden is.[30] 'Deep' verwijst naar het eerder behandelde 'deep learning' (zie hoofdstuk 5) en 'fake' naar nep. Deepfakes zijn onderdeel van een specifiek toepassingsgebied binnen AI: synthetische media.[31] Deze media worden onder andere gebruikt bij het ontwikkelen van videogames. De doorontwikkeling van AI heeft ertoe geleid dat het gebruik van synthetische media is verbreed naar meer domeinen.[32]

> *'We staan aan de vooravond van synthetische media. Binnen tien jaar kunnen programma's worden gepresenteerd door volledig kunstmatige personen, die vrijwel niet van echte mensen zijn te onderscheiden.[33] Nog eens tien jaar later manifesteren die kunstmatige personen zich aan ons als driedimensionale projecties. Wat echt is en wat schijn, is dan een kwestie van kosten, keuzes en voorkeuren.'*[34]

Experts verwachten dat het gebruik van deepfake-technologie de komende jaren een grote vlucht zal nemen.[35] Zij voorspellen dat in 2027 meer dan 90% van alle digitale content in meer of mindere mate is gemanipuleerd.[36] Met het blote oog zal het bijna onmogelijk zijn om vast te stellen of content een deepfake is. Deepfakes kunnen met zowel positieve als negatieve bedoelingen worden ingezet en beide zijn relevant voor het politiewerk.

> **Een deepfake van een slachtoffer**
>
> In mei 2022 publiceerde de politie in Nederland een deepfake van Sedar Soares.[37] Sedar werd in 2003 vermoord, terwijl hij samen met zijn vriendjes sneeuwballen gooide. In de video zie je hem met een voetbal onder zijn arm over een grasveld lopen. Dan staat hij stil en kijkt hij in de camera en zegt 'Weet jij meer? Spreek dan nu.' De video is bedoeld om nieuwe getuigen of eventueel de dader te bereiken. De achterliggende gedachte is dat een dergelijke video de kijker 'in het hart raakt' en daarmee meer effect heeft dan een andere vorm van communicatie. Het was een wereldprimeur in de opsporing.

30 Van der Sloot, Wagensveld & Koops 2021.
31 Duursma 2019.
32 Europol 2022a.
33 Hier is in India al sprake van. Zie ook hoofdstuk 5.
34 Klerks 2020.
35 Europol 2022a; Van der Sloot, Wagensveld & Koops 2021.
36 https://ibestuur.nl/artikel/hoe-temmen-we-de-fakes/ (voor het laatst geraadpleegd op 10 juli 2023).
37 https://www.politie.nl/nieuws/2022/mei/22/00-sedar-13-zoekt-zelf-zijn-moordenaar.html (voor het laatst geraadpleegd op 20 juli 2022).

Voor het veiligheidsvraagstuk aan de horizon zijn de negatieve bedoelingen het meest van belang. In verkenningen naar toekomstige dreigingen worden deepfakes steevast benoemd als fenomeen waar we ons veel zorgen over zouden moeten maken.[38] De deepfake-technologie kan voor uiteenlopende vormen van criminaliteit worden gebruikt.[39] Hierbij kan in de eerste plaats worden gedacht aan allerlei vormen van fraude. De vriend-in-nood of CEO-fraude die we nu kennen, is kinderspel vergeleken bij wat mogelijk is door gebruik te maken van deepfakes.

> **Voicecloning**[40]
> Marion uit Enschede krijgt op Hemelvaartsdag 2023 een telefoontje van haar zoon die volledig in paniek is. Hij is in Duitsland betrokken bij een motorongeluk en heeft een jonge moeder doodgereden. Vervolgens komt er een 'politieagent' uit Gronau aan de lijn die vertelt dat haar zoon niet wordt opgepakt als de uitvaartkosten direct worden betaald. Marion is in shock, maar schrikt nog meer als haar zoon tijdens het gesprek nietsvermoedend de woonkamer komt binnenlopen. De stem van jaar zoon is nagemaakt met AI. De oplichters vonden zijn stem online en hebben met AI-software getraind met zijn stem. Op basis van ingevoerde tekst kan de gebruiker van de software gesproken tekst produceren. Het gebruik van deze voicecloning voor fraude wordt ook wel *vishing* genoemd: voice phishing.[41]

Het gaat daarnaast om het genereren van deepfakes – zoals naaktfoto's en pornovideo's – die de mogelijkheid bieden om mensen te chanteren of reputatieschade toe te brengen (smaad of laster). In min of meer dezelfde categorie valt het genereren van kinderporno (zie ook de paragraaf over de metaverse). Een derde toepassing is het gebruik van deepfakes voor gezichtsherkenning bij online identificatie in het kader van toegang tot allerlei apparaten, bankaccounts, cryptoaccounts, online gokken en dergelijke. Kortom: biometrische kenmerken kunnen worden 'ge-deepfaked'. Tot slot: een van de meest zorgelijke doeleinden van deepfakes is het op grote schaal verspreiden van desinformatie met als oogmerk om haat te zaaien, aan te zetten tot geweld en/of democratische verkiezingen te beïnvloeden (zie het vorige hoofdstuk).[42] Met de opkomst van deepfakes gaat het verspreiden van desinformatie een nieuwe – meer zorgelijke – fase in.

Deepfakes resulteren vanuit het perspectief van de politie niet alleen in (nieuwe) vormen van criminaliteit en online ontsporingen, maar kunnen ook op andere manieren

38 Ciancaglini et al. 2020; Calwell et al. 2020; Europol 2022a.
39 Europol 2022a; Van der Sloot, Wagensveld & Koops 2021.
40 Gebaseerd op: https://www.rtvoost.nl/nieuws/2229400/vrouw-uit-enschede-bijna-opgelicht-met-nieuwe-levensechte-truc (voor het laatst geraadpleegd op 10 juli 2023). Zie ook: https://www.ad.nl/tech/belazerd-door-stem-van-huilende-dochter-afschuwelijk-dat-codetaal-met-je-kind-nodig-is (voorhet laatst geraadpleegd op 15 augustus 2023).
41 Europol 2023b.
42 Helmus 2022.

impact hebben op het politiewerk.[43] De politie kan op basis van gemanipuleerde content in actie komen, gemanipuleerde content kan worden gebruikt in opsporingsonderzoek (of authentieke content kan door aanpassingen als gemanipuleerd worden aangemerkt) en gemanipuleerde content kan worden gebruikt om politiemensen in een kwaad daglicht te zetten (en leiden tot doxing). Zo zijn er in internationaal verband al verschillende voorbeelden bekend van gemanipuleerd videomateriaal dat is ingebracht in strafrechtelijk onderzoek en strafrechtelijke vervolging.[44] Door deepfaketechnologie vervaagt de grens tussen waarheidsgetrouwe en artificiële representaties van gebeurtenissen. Dit belemmert het functioneren van de politie en het strafrechtelijke systeem als geheel.[45] Of, anders geformuleerd: het zorgt voor uitdagingen bij bewijswaardering.

Deepfakes worden op dit moment vooral ingezet voor desinformatie in het kader van polarisatie en interstatelijke vijandheden.[46] Daarnaast constateert de politie een groeiend aantal deepporn-incidenten.[47] Misbruik van deepfakes gaat zeer waarschijnlijk verder toenemen. Op dit moment is het maken van deepfake content vooral het werk van professionals.[48] Hoogwaardige deepfake content – het gaat dan in het bijzonder om video's – kan alleen worden gemaakt met kostbare hard- en software en veel trainingsdata. Dit gaat veranderen naarmate de benodigde hardware betaalbaarder wordt en de software geavanceerder.[49] ChatGPT is in dit verband een illustratie voor wat betreft het produceren van synthetische tekst en Midjourney voor synthetische afbeeldingen.[50] Voor synthetische videodata zijn er vanzelfsprekend ook applicaties beschikbaar, maar het produceren van 'echte nepvideo's' is simpelweg een grotere uitdaging. De dag dat eenieder op een app op de smartphone hoogwaardige deepfake video's kan maken, zal echter komen.[51] Het is een kwestie van tijd voordat het gebruik van deepfakes gemeengoed wordt bij het plegen van onder andere fraude, oplichting en misleiding. Op dat moment zal vooral de handhaving[52] in relatie tot deepfakes een uitdaging worden.[53]

43 Europol 2022a.
44 Zie bijvoorbeeld https://www.policechiefmagazine.org/law-enforcement-era-deepfakes/ (voor het laatst geraadpleegd op 20 juli 2022).
45 Europol 2022a; Van der Sloot, Wagensveld & Koops 2021.
46 Ciancaglini et al. 2020.
47 https://revu.nl/artikel/500333/grote-zorgen-over-kunstmatige-intelligentie-alles-nep-op-het-web (voor het laatst geraadpleegd op 31 juli 2023).
48 Helmus 2022.
49 Meer geavanceerde software wil vooral zeggen dat de GAN's verbeteren en het onderscheid tussen deepfakes en authentieke content steeds moeilijker kan worden gemaakt, ook door hoogwaardige detectiesoftware. Zie Helmus (2022).
50 In een rapport van het innovatielab van Europol (2023a) wordt erop gewezen dat het gebruik van ChatGPT kan worden gecombineerd met het gebruik van software voor het produceren van synthetische media, wat kan leiden tot risico's met betrekking tot deepfakes.
51 Helmus 2022.
52 Uit onderzoek blijkt dat het Nederlandse strafrecht goed is toegerust voor het aanpakken van deepfakes *die als strafwaardig* kunnen worden beschouwd. De meest problematische toepassingen van deepfakes zijn al verboden of juridisch ingekaderd. Zie hiervoor Van der Sloot, Wagensveld & Koops 2021.
53 Van der Sloot, Wagensveld & Koops 2021.

Criminaliteit in de metaverse

De derde en laatste categorie van digitale criminaliteit aan de horizon gaat over de ontwikkeling van de metaverse en heeft een sterk toekomstgericht karakter. De metaverse biedt – net als eerdere 'versies' van het internet – (nieuwe) mogelijkheden voor illegale en schadelijke gedragingen en praktijken.[54] Het gaat dan in de eerste plaats om bepaalde vormen van digitale criminaliteit, zoals identiteitsfraude, stelen van cryptovaluta, fraude met NFT's, stelen van data, fraude met *smart contracts* die een centraal onderdeel zijn van veel blokchaintechnologie en witwassen met gebruik van NFT's[55] en/of cryptovaluta (zie ook hoofdstuk 7). Welke risico's manifest worden, zal ook afhangen van de wijze waarop de metaverse wordt vormgegeven.

In de metaverse zal de interactie met anderen intiemer voelen dan die bij het huidige internet. De eerste onderzoeken naar *virtual reality* laten zien dat de gevoelde nabijheid tot andere gebruikers kan leiden tot het gevoel van intimidatie en aantasting van de persoonlijke ruimte.[56] Naarmate de metaverse meer realiteit wordt, komt er dus een meer fundamentele vraag op: hoe gaan we om met fysieke integriteit in een digitale wereld?[57] Wouter Stol merkt op dat naarmate een avatar meer voelt als een representatie van ons 'zelf', we harder geraakt zullen worden als onze avatar iets wordt aangedaan.[58] Het gaat dan niet alleen om geweld, maar ook om uitingen van haat, pesterijen en seksueel grensoverschrijdend gedrag. In eerste prototypes en voorlopers van 'de'[59] metaverse zijn de eerste tekenen hiervan al zichtbaar, bijvoorbeeld: vrouwen hebben melding gemaakt van seksueel grensoverschrijdend gedrag op een van de platformen van Meta.[60] Vooralsnog zijn al dit soort gedragingen in een virtuele wereld niet strafbaar. De enige uitzondering is virtuele kinderporno, dat in het Cybercrimeverdrag uit 2001 strafbaar is gesteld.[61] Dit betreft kinderpornografie die volledig met de computer is vervaardigd, zonder fysiek misbruik van kinderen (zie ook het vorige hoofdstuk). De wetgever heeft dit gedaan om te voorkomen dat er een sfeer ontstaat waarin seks met kinderen normaal is. Een dergelijke redenering kan worden verbreed. 'In het verlengde daarvan kan niet uitblijven dat om te beginnen virtuele aanranding en verkrachting onder het strafrecht worden gebracht, met in hun kielzog virtuele mishandeling en

54 Europol 2022b; Madiega, Car & Niestadt 2022.
55 Zie ook FIOD 2022.
56 Zie Roolvink, Kuijvenhoven & Huijstee 2022.
57 Madiega et al. 2022; Roolvink, Kuijvenhoven & Huijstee 2022; Schermer & Van Ham 2021.
58 Stol 2020; zie ook Roolvink, Kuijvenhoven & Huijstee 2022.
59 Dit staat tussen aanhalingstekens, omdat het vooralsnog gaat om verschillende werelden die los van elkaar staan. De metaverse ontstaat pas als deze werelden met elkaar worden verbonden.
60 https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/ (voor het laatst geraadpleegd op 20 juli 2022).
61 Zie Stol 2020.

moord', aldus Stol.[62] Of het 'niet kan uitblijven', weet ik niet, maar het is in ieder geval wel een vraagstuk dat zal gaan spelen.[63]

> *'… as the embodied internet is one of the ways of describing the metaverse, one can imagine that, as the technology gets more sophisticated, this crude delineation between physical and virtual will become increasingly problematic. As these experiences become more embodied, start to feel more real, we will have to decide at which point virtual experiences will be equally impactful as those of the physical realm. It will be important to have a clear idea of what is to be considered criminal behavior in the metaverse and to have matching laws to provide the means to prosecute these transgressions.'*[64]

Naast bedreigingen op het gebied van criminaliteit en onveiligheid biedt de metaverse de politie ook kansen, bijvoorbeeld op het gebied van contact met burgers en training.[65] Voor zowel de bedreigingen als de kansen geldt dat het voor de politie van belang is om tijdig te anticiperen.[66] Dit begint met het ontwikkelen van opvattingen over de eigen rol in en rondom de metaverse (zie ook hoofdstuk 20).[67] Met de behandeling van criminaliteit in het kader van de metaverse is het eerste deel van dit boek afgerond. We maken nu de stap van de invloed van technologie op het veiligheidsvraagstuk naar het gebruik van technologie in het politiewerk.

62 Stol 2020: 21. Zie ook https://www.nu.nl/tech/6184883/aanranding-bestaat-ook-in-virtual-reality-lijkt-echt-met-zon-bril-op.html (voor het laatst geraadpleegd op 20 juli 2022).

63 Het gaat hierbij zeker niet alleen om de virtuele daad zelf, maar ook om de vraag wat de impact is van immersieve ervaringen (via virtual of augmented reality in de metaverse) op ons gedrag in de fysieke wereld. Wordt iemand agressiever van een gewelddadige immersieve ervaring of gaat iemand seksueel grensoverschrijdend gedrag vertonen na het hebben van extreme virtuele seks (Schermer & Van Ham, 2021)?

64 Europol 2022b: 17.

65 Zie voor training in Nederland onder andere het werk van Bas Böing met betrekking tot het tegenaan van etnisch profileren (zie Böing & De Vries, 2021).

66 Europol 2022b.

67 Zie ook Roolvink, Kuijvenhoven & Huijstee 2022.

Deel III Technologiepraktijken

10 Selecteren van onderzoeken

Het is een dooddoener, maar daarmee niet minder waar: er is veel minder opsporingscapaciteit beschikbaar dan er potentiële opsporingsonderzoeken zijn.[1] Het gegeven dat de politie niet alles kan opsporen, impliceert dat er keuzes moeten worden gemaakt. Dit kiezen is aan de orde van de dag: er zijn binnen de politie allerlei selectieprocessen waarin, in afstemming met dan wel door het OM, keuzes worden gemaakt in welke zaken worden opgepakt.[2] In dit hoofdstuk wordt ingegaan op de rol die opkomende technologieën hierbij kunnen spelen.

Berekenen van kansrijkheid van zaken

Bij het selecteren van opsporingsonderzoeken worden op dit moment verschillende selectiecriteria gebruikt, zoals beleidsprioriteiten en de maatschappelijke impact van delicten. Hiermee wordt beoogd om tot een objectieve en rationele afweging te komen ten aanzien van voor welke opsporingsonderzoeken de schaarse capaciteit wordt ingezet. Een van de cruciale indicatoren is de kansrijkheid van de opsporing: hoe groot schatten we de kans in dat een opsporingsonderzoek tot opheldering van het misdrijf kan leiden? Het inschatten van de kansrijkheid is een doeleinde dat ook door (zelflerende) algoritmen kan worden gerealiseerd. De politie in Nederland heeft een prototype van een systeem ontwikkeld waarmee de kansrijkheid van *cold cases* kan worden ingeschat.

> **AI in cold cases**[3]
>
> In Nederland zijn er tien coldcaseteams die proberen om oude zaken – veelal moordzaken – alsnog op te lossen. Cold cases worden in de regel opgelost doordat getuigen met nieuwe informatie komen of forensische sporen die naar een verdachte wijzen.[4] Voor forensische sporen geldt dat er in de afgelopen decennia nieuwe analysetechnieken in gebruik zijn genomen die ten tijde van het initiële opsporingsonderzoek nog niet beschikbaar waren

1 De cryptocommunicatie (zie hoofdstuk 12) hebben deze situatie aanzienlijk versterkt waar het gaat om zogenaamde haalcriminaliteit. Overigens is de capaciteit in het vervolg van de strafrechtketen op het moment van schrijven – begin 2023 – een (nog) groter probleem dan de beschikbare opsporingscapaciteit.

2 Zie bijvoorbeeld Kouwenhoven & Kleijer-Kool 2016.

3 Deze inhoud is vooral gebaseerd op Kroes et al. 2023 en https://www.politie.nl/nieuws/2018/mei/23/00-nieuwe-technologie-in-oude-politiezaken.html (voor het laatst geraadpleegd op 4 augustus 2021). Zie ook https://thenextweb.com/news/how-the-dutch-police-is-using-ai-to-unravel-cold-cases (voor het laatst geraadpleegd op 12 juli 2023).

4 Van Leiden & Ferwerda 2006.

(zie ook hoofdstuk 11). Kortom: oude zaken kunnen met nieuwe technieken worden opgelost. De vraag is echter: welke oude zaken zijn het meest kansrijk, omdat ze sporen bevatten waarbij nieuwe technieken uitkomst kunnen bieden? Deze vraag is niet gemakkelijk te beantwoorden. Ik citeer een van de initiatiefnemers van het Q-LAB uit Oost-Nederland: 'We praten over een schatting van 25 miljoen pagina's in duizenden papieren dossiers. Want slechts 15 procent hiervan is gedigitaliseerd. Aan de buitenkant van al deze dossiers is niet te zien welke mogelijke kansrijke sporen ze bevatten. Om te bepalen of het zin heeft een zaak verder te onderzoeken maken forensisch rechercheurs daarom nu handmatig, per cold case, een sporenbeeld om dat te kunnen afzetten tegen de onderzoekstechnieken van vandaag. Dit duurt gemiddeld vijf tot dertig dagen. In het huidige tempo zijn we nog tientallen jaren bezig om de sporen in alle cold cases inzichtelijk te krijgen.'

Om sneller inzicht te krijgen in de kansrijkheid van cold cases is er een experiment uitgevoerd waarin gebruik wordt gemaakt van AI. Er is een systeem ontwikkeld – genaamd KEES – dat op basis van een algoritme de forensische sporen uit digitale dossiers selecteert en prioriteert. Het systeem is getraind om op basis van een gedetailleerd sporenbeeld een overzicht van alle (in het systeem opgenomen) cold cases te genereren, gerangschikt naar kansrijkheid of anders geformuleerd: verwachte oplosbaarheid. Het systeem bevat onder andere een filter waarmee de kansrijkheid van onvolledige DNA-profielen kan worden ingeschat. Bovenaan staat de zaak met de grootste kans om een verdachte te identificeren. De initiatiefnemers zien het als een hulpmiddel voor 'forensische (DNA) screening' en niet als vervanger van de rechercheur, al zal werk dat nu handmatig wordt uitgevoerd, worden geautomatiseerd (zie ook hoofdstuk 25). De verwachting is dat de politie hiermee sneller meer zaken kan oplossen. Het prototype van de software is opgeleverd en overgedragen aan de landelijke portefeuillehouder die voor de opgave staat om de technologie landelijk op te schalen.[5] Deze landelijke opschaling verloopt echter moeizaam (zie ook hoofdstuk 23).[6]

In het VK worden al tools ingezet voor actuele zaken. Het politiekorps in Kent – de bakermat van *intelligence-led policing* (ILP) – gebruikt een *evidence based investigation tool* (EBIT) waarmee de waarschijnlijkheid wordt berekend dat lichte geweldsmisdrijven en openbare orde-overtredingen kunnen worden opgehelderd.[7] Dit zijn veelvoorkomende feiten. Ieder type delict heeft een eigen algoritme – gebaseerd op weten-

5 De initiatiefnemers hebben de ambitie om naast DNA ook andere forensische sporen in het systeem te brengen en idealiter ook ander (dan forensisch) bewijs.
6 Kroes, Ter Veen & Kop 2023.
7 McFadzien et al. 2020.

schappelijk onderzoek naar factoren die van invloed zijn op de opheldering[8] – om zodoende de accuraatheid te vergroten. De tool adviseert aan welke zaken capaciteit voor verder onderzoek moet worden toegekend en welke zaken moeten worden 'afgeboekt'. De zaken die moeten worden afgeboekt, worden vervolgens beoordeeld op *public interest*. Hiervoor wordt een aantal kenmerken gebruikt, waaronder eerder slachtofferschap. Als een of meer van de betreffende *public interest* kenmerken aanwezig zijn, dan gaat de zaak naar een supervisor voor 'professionele beoordeling'. Deze supervisor bekijkt zowel de opheldering sscore als de kwalitatieve kenmerken van de zaak en bepaalt wat er met de zaak gebeurt. De uitkomsten van het opsporingsonderzoek (mate van opheldering) worden als feedback verwerkt, zodat de algoritmen kunnen worden verbeterd. De tool is zo ontworpen dat er – zonder dat de gebruikers dit weten – ook (dagelijks) één of twee zaken doorkomen die volgens de tool eigenlijk zouden moeten worden afgeboekt. Zo kan de accuraatheid van de algoritmen blijvend worden getest.

Uit onderzoek naar het gebruik van de tool komt naar voren dat de voorspelde opheldering skansen accuraat zijn: de zaken die de hoogste waarschijnlijkheidsscores krijgen, worden ook verhoudingsgewijs het vaakst opgelost. In een onderzoek naar de werking van de EBIT wordt het volgende geconcludeerd:

> *'By using EBIT, Kent Police has been able to improve the efficiency of their investigations into minor non-domestic assault and public order cases. The model employed does a very good job of prioritizing cases based on solvability, with those deemed most solvable demonstrably being solved at higher rates than those predicted to be less solvable. This demonstrated capacity to predict a detection is an advantage for police agencies wanting to prioritize cases that are reasonable uses of police time and resources. EBIT offers a substantial improvement in predictive accuracy over previous methods of allocation based on professional judgement alone or of allocating all cases for any high-volume offence category.'*[9]

Inmiddels zijn er meer politiekorpsen in het VK die gebruikmaken van deze en vergelijkbare slimme software.[10] Zo gebruikt het politiekorps in Norfolk in het VK een applicatie om de kans te berekenen dat opsporingsonderzoek naar een (woning)inbraak tot opheldering leidt.[11] Naast enthousiasme bij de betreffende politiekorpsen is er ook maatschappelijke kritiek: de politie zou zich door gebruik te maken van deze technologieën vooral richten op de gemakkelijk oplosbare zaken.[12] Bij deze kritiek moet wor-

8 Bijvoorbeeld: de snelheid waarmee het feit is gerapporteerd, aanwezigheid van forensische sporen en beschikbaarheid van bewijs op videobeelden. Overigens: dit is dus een expertsysteem (zie hoofdstuk 4).
9 McFadzien et al. 2020: 230.
10 Bland 2020.
11 https://www.dailymail.co.uk/news/article-6122341/Norfolk-Police-leave-computer-decide-worthwhile-investigating-burglary-cases.html (voor het laatst geraadpleegd op 8 oktober 2022).
12 Bland 2022; zie ook het artikel over Norfolk.

den opgemerkt dat de politie – ook zonder gebruik van algoritmen – keuzes maakt waarbij (gemakkelijke) oplosbaarheid een rol kan spelen. Dit nadeel is dus niet specifiek verbonden aan het gebruik van algoritmen voor het inschatten (voorspellen) van de oplosbaarheid.

Selectiviteit op het gebied van digitale criminaliteit
Als gevolg van veranderingen in de aard van de criminaliteit – van vooral fysieke naar steeds meer digitale criminaliteit – is het waarschijnlijk dat er meer nadruk komt te liggen op de selectiviteit in de opsporing van digitale criminaliteit. Het is tevens aannemelijk dat hiervoor technologie wordt benut. De eerste tekenen hiervan zijn al zichtbaar. Zo heeft de politie in Nederland een slimme keuzehulp ontwikkeld die burgers kunnen gebruiken bij het doen van aangifte van internetoplichting. Deze keuzehulp heeft onder andere tot doel om te voorkomen dat er onnodig aangifte wordt gedaan.[13]

Slimme keuzehulp aangifte internetoplichting[14]
Digitale aangiften van internetoplichting voldeden in het verleden geregeld niet aan alle bestanddelen van het delict. Na bestudering door politiemedewerkers bleek in die gevallen dat vooral opzet en/of valsheid ontbraken. Deze aangiften leveren de burger niets op en kosten de politie wel capaciteit. Om die reden is er een 'slimme keuzehulp' geïntroduceerd waar burgers gebruik van kunnen maken (je kunt ook direct aangifte doen). De eerste stap in het gebruik, is beschrijven wat je als burger hebt meegemaakt. Op basis hiervan zal het systeem veelal een aantal vervolgvragen stellen. Op basis van de situatiebeschrijving en de antwoorden op de vragen komt het systeem tot een advies. De keuzehulp gebruikt een combinatie van verschillende technieken – waaronder NLP – om de ingevoerde tekst te analyseren. Met behulp van een (regelgebaseerde) argumentatiemodule wordt vervolgens bepaald of er (op basis van de invoer) sprake is van internetoplichting. De regels in deze module zijn gebaseerd op het wetsartikel van oplichting. Als er sprake is van internetoplichting, dan kun je direct online aangifte doen. Indien dit niet het geval is, dan volgt er een ander advies. Een advies kan bijvoorbeeld zijn om nog even te wachten wanneer de kans aanwezig is dat een besteld product alsnog wordt geleverd of om contact op te nemen met een andere (door de keuzehulp) bepaalde partij, omdat het een civielrechtelijke kwestie is. Burgers weten zo sneller waar ze aan toe zijn en de politie kan zich concentreren op de aangiften van strafbare feiten. Burgers zijn over het algemeen behoorlijk tevreden over het gebruik van de keuzehulp. Het systeem is ontwikkeld in het Nationaal Politielab AI (zie hoofdstuk 23). De slimme keuzehulp leert – onder toezicht van politiemensen –

13 Deze keuzehulp heeft een ander karakter dan de hiervoor behandelde toepassingen om kansrijkheid te berekenen. Ik neem deze praktijk hier wel op, omdat het doel op hoofdlijnen hetzelfde is (selectiviteit).
14 https://www.politie.nl/nieuws/2019/september/26/sneller-duidelijkheid-bij-aangifte-internetoplichting.html (voor het laatst geraadpleegd op 4 januari 2023); zie ook De Kool, Vermeeren & Steijn 2020.

op basis van de invoer van burgers, zodat het systeem betere vragen kan stellen en antwoorden kan geven. De inzet van de slimme keuzehulp wordt vermoedelijk uitgebreid naar meer delicten.

De slimme keuzehulp wordt (dus) ingezet bij het intakeproces, voorafgaand aan het doen van aangiften. Op het moment dat aangifte van digitale criminaliteit wordt gedaan, is er een keuzemoment aan de zijde van de politie: pakken we de zaak op of niet? Dan wordt de vraag naar kansrijkheid relevant.[15] In verschillende eenheden wordt er op dit moment gebruikgemaakt van een 'cyberquery'.[16] Dit houdt in dat aangiften van gedigitaliseerde criminaliteit door de intelligenceorganisatie worden gescoord ten behoeve van de basisteams. Rood betekent dat een zaak met prioriteit moet worden opgepakt vanwege de heterdaad mogelijkheden. Oranje betekent dat het basisteam wordt geadviseerd om de zaak prioriteit te geven, omdat er opsporingsindicatie aanwezig is en groen wil zeggen dat het basisteam wordt geadviseerd om de zaak geen prioriteit te geven. De uitkomsten van de cyberquery worden dagelijks aangeboden aan de basisteams waar die worden bekeken door de casescreener, die de definitieve beslissing neemt en de eventuele start van het opsporingsonderzoek voorbereidt. Er zijn indicaties dat de cyberquery eraan bijdraagt dat de beschikbare opsporingscapaciteit wordt geïnvesteerd in minder, maar kansrijke zaken.

Een volgende stap is om de cyberquery door te ontwikkelen naar een slimme softwareoplossing die – op basis van inzicht in samenhang tussen kenmerken van (mogelijke) zaken en uitkomsten van opsporingsonderzoek naar digitale criminaliteit – berekent wat de kansrijkheid van zaken van digitale criminaliteit is. Deze stap kan echter alleen worden gezet als er voldoende data over (de aanpak van) digitale criminaliteit beschikbaar is, zodat algoritmen kunnen worden getraind dan wel een algoritme kan worden ontworpen (expertsysteem). Deze data zijn nu onvoldoende beschikbaar. Het is daarom van belang te werken aan een verbeterde, landelijke informatiehuishouding op het gebied van digitale criminaliteit in het algemeen en gedigitaliseerde criminaliteit in het bijzonder.[17]

15 Inzicht in de kansrijkheid is bij de aanpak van digitaliseerde criminaliteit in de basisteams vermoedelijk 'extra relevant', omdat er in basisteams sprake kan zijn van terughoudendheid om aan de opsporing van zaken van gedigitaliseerde criminaliteit te beginnen, omdat men de indruk of ervaring heeft dat dit niet of moeizaam tot opheldering leidt (zie Kort & Spithoven, 2021).

16 Schiks, van 't Hoff-de Goede & Leukfeldt 2022.

17 Kort & Spithoven 2021.

11 Uitvoeren van DNA-onderzoek

Forensisch opsporingsonderzoek heeft van oudsher het karakter van onderzoek naar fysieke sporen, die kunnen leiden tot *tangible evidence*: aanraakbaar bewijs.[1] De (fysieke) forensische opsporing verandert onder invloed van digitalisering. Dit wil onder andere zeggen dat er steeds meer (referentie)databases zijn waarmee aangetroffen sporen steeds sneller kunnen worden vergeleken om zodoende snel vast te stellen of de donor van het spoor 'bekend' is bij de politie. In dit hoofdstuk beperk ik me tot enkele technologische ontwikkelingen met betrekking tot DNA-onderzoek. Deze ontwikkelingen zijn – tot op zekere hoogte – illustratief voor de bredere ontwikkelingen op het gebied van (fysiek) forensisch opsporingsonderzoek.

Bijdrage van DNA aan opsporingsonderzoek
Mensen, planten en dieren zijn opgebouwd uit cellen en in elke cel ligt een celkern met chromosomen; dit zijn de dragers van de erfelijke eigenschappen.[2] De chromosoomstructuur van ieder mens is – met uitzondering van eeneiige meerlingen – uniek. Kortom: ieder mens is in genetisch opzicht uniek. Chromosomen zijn opgebouwd uit DNA: een lang molecuul dat bestaat uit stukjes met kenmerkende structuren die op vaste plaatsen op het molecuul liggen. Een deel van dit DNA kan worden gebruikt om een DNA-profiel van een individu te bepalen. Een DNA-profiel heeft een zeer groot persoonsonderscheidend vermogen. Daarnaast geldt dat mensen gemakkelijk biologisch celmateriaal – zoals huidcellen, speeksel, bloedcellen – achterlaten op plaatsen waar zij handelingen hebben verricht.

De combinatie van bovenstaande kenmerken zorgt ervoor dat DNA-onderzoek een belangrijke bijdrage kan leveren aan het reconstrueren en bewijzen van strafbare feiten.[3] Als het profiel van een aangetroffen spoor niet overeenkomt met het DNA-profiel van een persoon, dan kan deze persoon worden uitgesloten als donor van dit spoor. Een overeenkomst wil niet direct zeggen dat de persoon de donor is van het spoor,

1 Zie Van Koppen (2022) voor deze term. Hij stelt overigens dat bewijs niet 'aanraakbaar' kan zijn, omdat het 'ding' zelf (bijvoorbeeld een wapen) niets kan bewijzen. Het gaat om het verhaal over het pistool in relatie tot het gepleegde delict.

2 Deze alinea is gebaseerd op De Poot (2021). Voor een uitgebreide toelichting op forensisch DNA-onderzoek wordt verwezen naar Meulenbroek (2021).

3 Met betrekking tot het reconstrueren van strafbare feiten wordt vaak onderscheid gemaakt tussen de zeven W-vragen: *wie* kan in verband worden gebracht met het strafbaar feit, *wat* is er gebeurd, *waar* is het gebeurd, *wanneer* is het gebeurd, *waarmee* is het misdrijf gepleegd, *op welke wijze* is het misdrijf gepleegd en *waarom* is het misdrijf gepleegd (zie De Poot et al. 2004).

maar als er sprake is van een volledig profiel, dan is de kans dat een willekeurige persoon – niet zijnde familie van de donor – hetzelfde DNA-profiel heeft als het aangetroffen spoor altijd kleiner dan 1 op 1 miljard. Hierbij moet worden benadrukt dat DNA niet enkel een verdachte kan in- of uitsluiten als mogelijke donor van een spoor, maar tevens informatie bevat die kan worden gebruikt om kenmerken van de donor – zoals geslacht en uiterlijke kenmerken – te achterhalen waarmee richting kan worden gegeven aan een opsporingsonderzoek en de daarin opgestelde hypothesen en scenario's.

> *'Het is fascinerend dat iets wat je niet kunt zien, horen, ruiken, voelen of proeven, zo cruciaal kan zijn voor het oplossen van misdrijven.'*[4]

Sinds 1997 is er in Nederland een DNA-databank voor strafzaken. Eind 2021 waren er ongeveer 360.000 personen in de databank opgenomen.[5] Het DNA-profiel dat (idealiter) het onderzoeksresultaat is van aangetroffen sporen kan worden vergeleken met de DNA-databank. Op dit moment levert dit per week zo'n 85 spoor-persoonmatches op.[6] Hierbij moet worden opgemerkt dat DNA-onderzoek in de huidige situatie vooral een bijdrage levert aan bewijs in strafzaken.[7] Aan de voorkant van het opsporingsproces – waaronder het identificeren van onbekende verdachten – is de rol van DNA vooralsnog gering(er).[8] Dit heeft verschillende oorzaken, waaronder het gegeven dat niet bij ieder misdrijf voldoende (bruikbare) sporen worden gevonden die leiden tot een DNA-profiel en het feit dat DNA-onderzoek nog steeds veel tijd in beslag neemt, waardoor de resultaten relatief laat in het opsporingsproces beschikbaar komen.[9] Technologische ontwikkelingen bieden (in potentie) oplossingen voor deze knelpunten.[10] Ik beperk me hier tot drie innovaties met opkomende technologieën: DNA-succesmeter, snelle identificatielijn en mobiele DNA-analyse.

DNA-succesmeter

DNA-onderzoek begint met het aantreffen van (biologische) sporen.[11] Het is weliswaar mogelijk om uit zeer geringe hoeveelheden sporenmateriaal goede DNA-profielen af te leiden, maar die sporen moeten dan wel worden gevonden. Dit is een uitdagende opgave, in het bijzonder bij sporen die niet goed zichtbaar zijn. Wanneer (kleine hoeveelheden) sporenmateriaal met het blote oog niet zichtbaar zijn, is men aangewezen op het 'blind' bemonsteren van plekken – bijvoorbeeld een deurklink – waar kan worden verwacht dat sporen kunnen worden aangetroffen. Rechercheurs blijken echter geen goed beeld te hebben van de kans dat ze op bepaalde sporendragers/plekken

4 Meulenbroek 2021: 25.
5 Meulenbroek 2021.
6 Idem.
7 De Poot 2021.
8 Het gaat dus om geringer. Talloze matches in de DNA-databank (voor strafzaken) hebben geleid tot identificatie van verdachten, bijvoorbeeld in cold cases. Zie Meulenbroek (2021).
9 De Poot 2021. Zie voor de lange duur ook: Mapes 2017; Van Wijk, Van Leiden & Hardeman 2017.
10 Mapes 2017; De Poot 2017, 2021.
11 Deze alinea is gebaseerd op: De Poot 2021.

sporen zullen aantreffen.[12] Zo blijven veel kansrijke sporen achter op de PD en tegelijkertijd worden er sporen opgestuurd voor DNA-onderzoek die geen bruikbare DNA-profielen opleveren, maar waarbij wel een beroep wordt gedaan op – vooralsnog – schaarse analysecapaciteit.[13] Een van de innovaties die kan bijdragen aan een oplossing voor dit probleem is de DNA-succesmeter.

DNA-succesmeter[14]

De DNA-succesmeter is een beslissingsondersteunend systeem waarin inzichten over de succeskansen van sporen zijn opgenomen. Deze inzichten zijn gebaseerd op gegevens uit eerder strafrechtelijk en wetenschappelijk onderzoek. Het achterliggende idee is dat rechercheurs en analisten hun beslissingen over het veiligstellen van sporendragers, het bemonsteren hiervan en de inzet van specifieke analysetechnieken (zie het vervolg van dit hoofdstuk) kunnen baseren op de resultaten van eerdere ervaringen die hiermee zijn opgedaan in forensisch onderzoek. Het systeem moet op deze wijze helpen om op de PD doordachtere keuzes te maken. De DNA-succesmeter maakt gebruik van big data-technieken om de data uit de systemen van de politie en het Nederlands Forensisch Instituut (NFI) te categoriseren en dit is (vooralsnog) zeer arbeidsintensief. Het prototype van het systeem beperkt zich op dit moment tot inzichten over de kans dat een spoor tot een DNA-profiel leidt. Dit is waardevol, maar de ambitie is om ook inzichten te kunnen verschaffen over de relevantie van een spoor. Dit zou de doordachtheid van keuzes verder kunnen bevorderen. Een spoor van het slachtoffer op diens eigen kleding kan immers wel tot een goed DNA-profiel leiden, maar dat is niet zo relevant. Vooral een spoor van de verdachte op de kleding van het slachtoffer is relevant. Het is vooralsnog niet gelukt om door middel van big data-technieken het gebrek aan eenduidige registratie te overwinnen (wat nodig is om data over relevantie van sporen te kunnen categoriseren en relateren). Het arbeidsintensieve karakter van het categoriseren (voor succeskansen) maakt ook dat het systeem op dit moment niet wordt geactualiseerd met nieuwe gegevens. Als de partijen in de strafrechtketen hun gegevens volledi ger, betrouwbaarder en eenduidiger gaan registreren, ontstaan nieuwe kansen voor de DNA-succesmeter als beslissingsondersteunend systeem voor DNA-onderzoek. Hier wordt aan gewerkt.

12 Mapes 2017.
13 Idem.
14 Gebaseerd op: De Poot 2021; Zuidberg et al. 2018.

Snelle identificatielijn

Een tweede ontwikkeling betreft het automatiseren van het proces van een (eenvoudig[15]) spoor tot en met de DNA-rapportage.[16] Het NFI heeft als eerste forensisch instituut in de wereld software ontwikkeld die dit mogelijk maakt. De volgende stappen worden geautomatiseerd uitgevoerd: analyseren van het DNA-spoor, interpreteren van het DNA-profiel, vergelijken met personen binnen de zaak, (eenmalig) vergelijken met data in de DNA-databank voor strafzaken[17] en de rapportage. De doelstelling is dat de politie en het OM drie werkdagen na het insturen van een spoor weten of er een overeenkomst is met het DNA-profiel van een persoon in de zaak of met een persoon in de DNA-databank. Het betreft nog geen volledig rapport; dat volgt later alsnog. De verwachting is dat de snelle beschikbaarheid van de uitkomsten ertoe leidt dat de opsporing gerichter stukjes van de puzzel in het onderzoek kan leggen of bepaalde scenario's in het onderzoek kan uitsluiten.

In het najaar van 2021 is gestart met een proeftuin waarin het geautomatiseerde proces – genaamd de Snelle ID-lijn – wordt gebruikt. Er is gedurende tien maanden onderzoek verricht naar de resultaten van het geautomatiseerde proces en deze zijn vergeleken met het reguliere, handmatige proces.[18] Hieruit komt naar voren dat de Snelle ID-lijn daadwerkelijk veel sneller is dan het handmatige, reguliere proces: in ruim 75% van de zaken was het mogelijk om de resultaten binnen drie werkdagen terug te koppelen. Daarnaast heeft het geautomatiseerde proces in een klein deel van de gevallen geleid tot een match die niet direct uit het reguliere proces naar voren kwam. Dit komt doordat in het automatische proces complexe sporen eenmalig worden vergeleken met de DNA-databank. Dit gebeurt in het handmatige proces niet meteen, omdat dit capaciteit kost. Het NFI is vanaf eind 2022 het geautomatiseerde proces gaan inzetten voor alle sporen die door de politie worden ingestuurd voor DNA-profilering, analyse en interpretatie. Het streven is om de geautomatiseerde werkwijze uit te breiden naar ingewikkelde DNA-mengprofielen.

Mobiele DNA-analyse

Dan tot slot: mobiele DNA-identificatietechniek, ook wel mobiele DNA-analyse genoemd. Deze technologie heeft het karakter van zogenaamde *lab-on-chip technologie*: verschillende meet- en analysefuncties zijn geïntegreerd in één chip. Hierdoor wordt het mogelijk om de analyse van bepaalde DNA-sporen te verplaatsen van het laboratorium naar de PD (of een andere locatie).[19] In Nederland zijn met het uitproberen van deze technologie in de afgelopen jaren eerste stappen gezet. Met een mobiel apparaat

15 DNA-mengprofielen moeten nog door mensen worden geanalyseerd.
16 Deze alinea is gebaseerd op: https://www.forensischinstituut.nl/actueel/nieuws/2021/11/08/misdrijven-sneller-oplossen-dankzij-automatisering-van-dna-proces-van-a-tot-z-bij-het-nfi (voor het laatst geraadpleegd op 29 december 2021).
17 Zie Meulenbroek (2021) voor een uitgebreide toelichting op de DNA-databank.
18 Benschop et al. 2022.
19 De Gruijter 2017; Mapes 2017; De Poot 2017, 2021.

wordt DNA-data uit sporen gegenereerd en deze data worden vergeleken met de data in de DNA-databank voor stafzaken. De huidige technologie maakt mobiele DNA-analyse mogelijk voor relatief grote bloed- en speekselsporen. De technologie is namelijk minder gevoelig dan de apparatuur die vooralsnog in het laboratorium wordt gebruikt voor DNA-onderzoek (en dus heb je relatief grote sporen nodig).[20]

Het gebruik van mobiele DNA-analyse is eerst uitgeprobeerd in experimenten (gecontroleerde omgevingen)[21] en vervolgens – na invoering van het nieuwe DNA-besluit[22] – gebruikt in praktijkproeftuinen[23] in Amsterdam en Midden-Nederland.[24] In de praktijkproeftuinen wordt voor het forensisch onderzoek gebruikgemaakt van een speciale bus: de *Forensic Identification Vehicle* (FIV). De eerste experimenten en praktijkproeftuinen geven een relatief eenduidig beeld. De technologie zorgt ervoor dat forensisch onderzoek zich verplaatst naar de voorkant van het opsporingsproces en geeft daarmee ook meer richting aan het opsporingsonderzoek.[25] De uitkomsten van DNA-onderzoek komen namelijk veel sneller in het proces terecht en kunnen direct worden gebruikt. De *turnaround time* gaat van weken of dagen naar één tot twee uur.[26] Waar (informatie)processen voorheen een sequentieel karakter hadden, verloopt het nu meer parallel en geïntegreerd. Dit wil zeggen dat tactisch en forensisch meer gelijktijdig en gezamenlijk optrekken. Dit heeft een motiverend effect op rechercheurs, omdat zij sneller op de uitkomsten van DNA-onderzoek kunnen acteren.[27]

Een deel van de opsporingsonderzoeken[28] kan met behulp van mobiele DNA-analyse sneller succesvol worden afgerond.[29] Daders kunnen sneller worden aangehouden en seriematige delicten kunnen (hierdoor) worden doorbroken.[30] Daarnaast hoeven andere opsporingsmethoden in een deel van de gevallen – in vergelijking met voorheen – niet meer te worden ingezet.[31] De tijdwinst kan alleen worden gerealiseerd als er in het gehele werkproces voldoende capaciteit aanwezig is en de uitkomsten van de snelle

20 Mapes 2017; De Roo & De Poot 2022.
21 De Gruijter 2017; Mapes 2017.
22 Waarmee de mogelijkheid van DNA-onderzoek met mobiele apparatuur werd geïntroduceerd.
23 De proeftuin heet Local DNA en is inmiddels afgerond.
24 De Poot 2021; De Roo & De Poot 2022.
25 Het gaat overigens om meer dan de technologie. Het betreft ook een nieuw werkproces met nieuwe rollen en taken van ketenpartners, een beslissingsondersteunend systeem (zie ook de DNA-succesmeter) en een kwaliteitsondersteunend systeem (zie De Roo & De Poot, 2022).
26 De Gruijter 2017.
27 De Roo & De Poot 2022.
28 De huidige manier van werken met betrekking tot (snelle) mobiele DNA-analyse is potentieel inzetbaar voor 3 à 4% van alle zaken die door FO worden onderzocht. Als de potentiële inzet van de manier van werken wordt gerelateerd aan het aantal zaken waarin DNA-sporen worden veiliggesteld op de PD en bloed en/of speeksel wordt geselecteerd voor DNA-onderzoek, dan gaat het om 9 à 11% van de maatwerk(+)/TGO-zaken en 19-33% van de standaardzaken (dit verwijst naar een categorisering van zaken die binnen het OM wordt gebruikt).
29 Mapes 2017.
30 De Roo & De Poot 2022.
31 Mapes 2017.

DNA-analyse direct worden benut door het onderzoeksteam.[32] Hierbij is de wijze van gebruik door het onderzoeksteam een aandachtspunt. De snelle beschikbaarheid van uitkomsten van DNA-onderzoek draagt idealiter bij aan de reconstructie van het misdrijf. De eerste ervaringen in met name de experimenten laten echter zien dat er bij rechercheurs een sterke focus kan blijven bestaan op het vinden van de verdachte, de zogenaamde *who done it routine*.[33]

De snelle (mobiele) DNA-analyse is veelbelovend. Op dit moment is het echter nog niet mogelijk om de nieuwe manier van werken standaard in het opsporingsproces te integreren.[34] Er is nader onderzoek nodig om goed te kunnen bepalen in welke zaken en omstandigheden de technologie wel en niet kan worden ingezet. Hiermee samenhangend moet ook worden bepaald welke specifieke technologie het meest geschikt is.[35] Daarnaast spelen er allerlei kwaliteitseisen en juridische waarborgen waarmee snelle DNA-analyse op locatie is omgeven, waaronder certificering van personeel. Er zijn tot slot organisatorische afwegingen aan de orde, waaronder de inzettijden van deze manier van werken – 24/7 of tijdens 'kantoortijden' – en financiële investeringen die nodig zijn.

Tot slot. Er zijn hobbels te overwinnen, maar het DNA-onderzoek in het politiewerk aan de horizon zal hoe dan ook bepalender worden aan de voorkant van het opsporingsproces. DNA-onderzoek gaat meer – dan op dit moment het geval is – bijdragen aan het opbouwen van het verhaal over het misdrijf en het identificeren van de mogelijke dader.[36] Deze ontwikkeling naar de voorkant van het opsporingsproces – die (mede) mogelijk wordt gemaakt door digitale technologie – geldt breder voor het (fysiek) forensisch onderzoek.[37] Het is waarschijnlijk dat de effectiviteit (opheldering) en efficiëntie (selectiviteit in inspanningen) van het opsporingsproces hierdoor zullen verbeteren (zie ook hoofdstuk 26).

32 De Roo & De Poot 2022.
33 De Gruijter 2017; Mapes 2017.
34 De Poot 2021; zie ook De Roo & De Poot 2022.
35 De proeftuinen zijn uitgevoerd met de RapidHIT ID. Er zijn ook andere apparaten voor snelle DNA-analyse mogelijk waarbij de mate van mobiliteit kan verschillen. Zie verder De Roo & De Poot (2022).
36 De Poot 2021.
37 Het gaat *bijvoorbeeld* niet alleen om het snel vergelijken van DNA-profielen, maar ook om dactyloscopische gegevens (vingerafdrukken). Deze gegevens zijn opgenomen in Het Automatisch Vingerafdrukkensysteem Nederlandse Kollektie (HAVANK). De inmiddels vierde editie van dit systeem heeft een verbeterd zoekalgoritme, zodat de kans dat sporen in de database worden gevonden wordt verhoogd. Politiemedewerkers kunnen met een app – plaats delict onderzoek (Ter Veen & Kop, 2021) – een vingerafdruk nemen en deze kan snel worden vergeleken met de gegevens in HAVANK.

12 Cryptocommunicatiedata

Een van de meest betekenisvolle innovaties die er – naar mijn idee – in de afgelopen tien tot twintig jaar heeft plaatsgevonden in de opsporing van de georganiseerde criminaliteit is de interceptie van zogenaamde cryptocommunicatiedata. Dit hoofdstuk gaat op hoofdlijnen in op de *cryptotelefoonoperaties* die hebben plaatsgevonden en de veranderingen die deze teweeg hebben gebracht in de manier van werken in de opsporing.

Cryptotelefoonoperaties

Ennetcom als start van een nieuwe manier van opsporen
Op 17 april 2016 werd in IJsselstein een man doodgeschoten.[1] De verdachte werd in de nabijheid van de PD aangehouden op verdenking van moord. Kort na zijn aanhouding werden BlackBerry telefoons aangetroffen. Deze BlackBerry's waren geprepareerd, zodat ze alleen versleutelde berichten konden versturen. Ennetcom was de Nederlandse dienstverlener voor deze versleutelde Pretty Good Privacy (PGP)-communicatie. De berichten werden door Ennetcom opgeslagen op servers in Canada. Door de politie in Nederland is een rechtshulpverzoek aan Canada ingediend in het kader van vier lopende opsporingsonderzoeken. Het verzoek was om alle beschikbare gegevens van de betreffende servers over te dragen. De Canadese rechter heeft naar aanleiding hiervan beslist dat de gegevens aan Nederland konden worden overgedragen ten behoeve van de vier onderzoeken en ten behoeve van andere onderzoeken. Hierbij is als voorwaarde gesteld dat er voorafgaand aan het gebruik in een onderzoek een machtiging van een Nederlandse rechter nodig is. Deze 'Ennetcomdata' bestonden uit ongeveer 3,6 miljoen versleutelde berichten van criminelen, bij elkaar zo'n 7 terabyte. De versleutelde berichten zijn gekraakt met encryptiesleutels die op de servers zijn veilig gesteld. Met behulp van software – genaamd Hansken – zijn de

1 Deze passage is gebaseerd op:
https://www.hogeraad.nl/actueel/nieuwsoverzicht/2022/juni/hoge-raad-zogenoemde-ennetcomdata-mogen-gebruikt-bewijs (voor het laatst geraadpleegd op 28 juli 2022);
https://nos.nl/artikel/2162140-om-3-6-miljoen-versleutelde-berichten-van-criminelen-gekraakt (voor het laatst geraadpleegd op 28 juli 2022);
https://jjoerlemans.com/2020/03/09/ai-strafrecht-en-het-recht-op-een-eerlijk-proces (voor het laatst geraadpleegd op 28 juli 2022).

> data doorzocht en geanalyseerd (zie hoofdstuk 13). Hierbij is gebruikgemaakt van bepaalde zoektermen die onder andere te maken hebben met drugstransporten.[2] Het doorzoeken van de data heeft geleid tot subsets die – met toestemming van de rechter-commissaris – in andere opsporingsonderzoeken zijn gebruikt. De data uit de berichten zijn op deze wijze gebruikt als bewijs in tientallen opsporingsonderzoeken naar drugshandel, witwassen, pogingen tot moord, liquidaties en andere vormen van georganiseerde criminaliteit. De oprichters van Ennetcom zijn veroordeeld voor deelname aan een criminele organisatie, witwassen en het medeplegen van valsheid in geschrifte.

Ennetcom was het begin van een serie cryptotelefoonoperaties die in de afgelopen jaren hebben plaatsgevonden.[3] Dit zijn:[4]

- Ennetcom (2017).
- PGP-safe (2017).
- IronChat (2018).
- EncroChat (2020).
- Sky ECC (2021).
- ANOM (2021).
- Exclu (2023).

Het zijn allemaal (internationale) operaties gericht op het verkrijgen van versleuteld berichtenverkeer, maar er zijn verschillen in omvang en wijze waarop het berichtenverkeer is verkregen.[5] De meest omvangrijke operaties zijn vanuit Nederlands perspectief EncroChat en Sky ECC. Deze worden hierna kort toegelicht waarbij allerlei relevante details niet worden vermeld.[6]

---

2 Hirsch Ballin & Oerlemans 2023.

3 Zie ook https://jjoerlemans.com/2022/11/14/overzicht-cryptophone-operaties voor een overzicht van de cryptotelefoonoperaties (voor het laatst geraadpleegd op 1 januari 2022).

4 Het jaartal verwijst naar het jaar waarin de operatie naar buiten is gebracht. Voor verschillende operaties geldt dat deze eerder zijn gestart. Het gaat dan vooral om het opsporingsonderzoek naar de eigenaren c.q. beheerders van de cryptocommunicatiedienst (dat bij de latere operaties moet worden onderscheiden van het opsporingsonderzoek naar de gebruikers).

5 ANOM is de meest afwijkende operatie. In 2018 is er door het Federal Bureau of Investigation (FBI) van de VS een man aangehouden die op het punt stond om met een nieuwe cryptotelefoondienst – ANOM – de criminele markt op te stappen. In ruil voor strafvermindering is hij gaan werken als burgerinfiltrant en ANOM verder gaan ontwikkelen en distribueren. De cryptotelefoondienst groeide uit tot meer dan twaalfduizend toestellen die zijn gebruikt door meer dan driehonderd criminele netwerken in meer dan honderd landen. Vooral na inbeslagname van de servers van Sky ECC nam de verkoop van de ANOM-dienst een grote vlucht. De FBI heeft samen met zestien (andere) landen – waaronder Nederland – anderhalf jaar kunnen meelezen met in totaal zo'n 27 miljoen berichten (en foto's) met als voordeel dat deze niet ontsleuteld hoefden te worden. Dit heeft onder ander geleid tot een omvangrijke internationale operatie in juni 2021: operatie Trojan Shield/OTF Greenlight (FBI/Europol). Hierbij zijn ruim achthonderd criminelen aangehouden. Zie voor een verdere uitwerking: Taylor Parkins-Ozephius et al. 2021.

6 Zie voor details onder andere het werk van Jan-Jaap Oerlemans. Op zijn website is veel informatie te vinden.

De dienstverlening van EncroChat kwam aan het licht toen in verschillende strafrechtelijke onderzoeken EncroChat telefoons werden aangetroffen.[7] Als gevolg hiervan ontstond bij de politie de indruk dat deze telefoons vrijwel uitsluitend in het criminele circuit werden gebruikt. In zowel Frankrijk als Nederland werd in 2017 een strafrechtelijk onderzoek gestart naar het bedrijf EncroChat van wie de server bij het bedrijf OVH in Roubaix in Frankrijk was gevestigd.[8] Het onderzoek – dat in Nederland de codenaam '26Lemont' meekreeg – was gericht op medeplichtigheid van EncroChat aan de door gebruikers gepleegde misdrijven. Nederland en Frankrijk hebben het voortouw genomen bij het opzetten van een Joint Investigation Team (JIT) tussen verschillende landen. Door het JIT is er interceptiesoftware ontwikkeld[9] die vervolgens door de Franse politie heimelijk via een update op de telefoons van alle vijftigduizend gebruikers is geïnstalleerd.[10] De software stuurde gegevens door naar de Franse autoriteiten (waaronder gebruikersnaam, opgeslagen berichten, afbeeldingen, locatiegegevens), die vervolgens werden gedeeld in het JIT. Op deze wijze konden de politiediensten van een groot aantal landen tussen 1 april en medio juni 2020 live meelezen met het berichtenverkeer van de EncroChat gebruikers en daarnaast historische data kopieren.[11] De operatie heeft in totaal geleid tot onderschepping van zo'n 25 miljoen berichten die relevant zijn voor Nederland.

Sky ECC was een Canadese aanbieder van cryptotelefoons met ongeveer 11.000 gebruikers in Nederland.[12] In een internationaal onderzoek naar een crimineel samenwerkingsverband – dat in 2018 in Amsterdam startte – stuitte men op versleutelde communicatie via telefoons van Sky ECC. In verschillende landen zijn opsporingsonderzoeken naar de aanbieder van Sky ECC gestart. De Franse autoriteiten hebben in hun onderzoek een – door specialisten van de politie in Nederland ontwikkelde – interceptietool ingezet, waarvoor een Franse onderzoeksrechter een machtiging heeft verleend.[13] Met deze tool zijn vervolgens data van de toestellen van Sky ECC verzameld. Deze data zijn gedeeld met Nederland en België in het kader van een JIT gericht op de verdenkingen tegen Sky ECC en de vermeende criminele samenwerkingsverbanden die van Sky ECC gebruikmaken. In Nederland is het onderzoek '26Argus' gestart, gericht op de criminele samenwerkingsverbanden van de Nederlandse gebruikers. Er is drie weken live meegelezen met de berichten. Daarnaast zijn eerder

7 Zie Schermer & Oerlemans 2022.

8 Zie voor details ook: https://www.computerweekly.com/news/366542786/Three-years-on-EncroChat-cryptophone-hack-nets-6500-arrests-and-seizures-of-900-million (voor het laatst geraadpleegd op 13 juli 2023).

9 De Nederlandse politie heeft hierin – naar het schijnt – een grote rol gespeeld.

10 Zie ook https://jjoerlemans.com/2021/07/06/meer-duidelijkheid-over-encrochat-operatie (voor het laatst geraadpleegd op 22 oktober 2021).

11 Bij IronChat kon de politie voor het eerst enige tijd live meelezen met het berichtenverkeer. Zie hiervoor https://www.parool.nl/nieuws/weer-een-server-gekraakt-maar-criminelen-blijven-chatten (voor het laatst geraadpleegd op 28 juli 2022).

12 https://www.nrc.nl/nieuws/2021/03/09/blauwdruk-onderwereld-ligt-bloot (voor het laatst geraadpleegd op 17 augustus 2021).

13 https://jjoerlemans.com/2022/09/05/cybercrime-jurisprudentieoverzicht-september-2022 (voor het laatst geraadpleegd op 8 oktober 2022).

verzonden berichten 'ontsleuteld'.[14] Hiervan zijn er in ieder geval 80 miljoen relevant voor Nederland.

Gamechanger in de opsporing

Het live meelezen met de versleutelde berichten die criminelen elkaar stuurden, was – mede gegeven de schaal waarop dit plaatsvond – een unieke gebeurtenis in de opsporing. Bij de internationale persconferentie naar aanleiding van de EncroChat-operatie formuleerde toenmalig politiechef van de landelijke eenheid Jeanine van de Berg dit als volgt: 'Het was alsof we aan de vergadertafel van de criminelen zaten mee te luisteren.'[15] Deze beeldspraak geeft een indruk van de informatiepositie van de politie tijdens de livefase, maar is tegelijkertijd enigszins misleidend. Om in de beeldspraak te blijven: het gaat om ontelbare vergadertafels waaraan criminelen met elkaar communiceren. Tijdens de livefase ontstond dus de vraag hoe ervoor kon worden gezorgd dat de meest relevante communicatie onder ogen van opsporingsambtenaren kwam, zodat er (direct) kon worden gereageerd op dreigende situaties, waaronder liquidaties. AI bood uitkomst.

Interveniëren voordat liquidaties plaatsvinden

Door het Nederlands Forensisch Instituut (NFI) is – op het al bestaande platform Hansken (zie hoofdstuk 13) – een model ontwikkeld waarmee kan worden voorspeld welke berichten uit de cryptocommunicatiedata een serieuze bedreiging bevatten.[16] Het model maakt gebruik van *deep learning*. Medewerkers van het NFI 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 – met tienduizenden bedreigende en niet-bedreigende zinnen – getraind door medewerkers van het NFI.[17] De politie heeft het model vervolgens ingezet en de resultaten gecontroleerd (feedback aan het model). Zo werd de software steeds

14 Om een indruk van de omvang te geven: twee jaar na de Sky ECC-operatie zijn er 1 miljard berichten ontsleuteld en dit proces is nog steeds gaande. Zie https://www.ad.nl/binnenland/het-maakt-niet-meer-uit-in-welk-land-criminelen-zich-schuilhouden-recherche-heeft-sleutelrol-in-de-wereld (voor het laatst geraadpleegd op 14 juli 2023).

15 https://www.parool.nl/nederland/recherche-slaat-enorme-slag-met-kraken-25-miljoen-berichten (voor het laatst geraadpleegd op 17 augustus 2021).

16 https://www.forensischinstituut.nl/actueel/nieuws/2021/05/05/nfi-leert-computers-om-berichten-met-doodsbedreiging-uit-grote-hoeveelheden-data-te-filteren (voor het laatst geraadpleegd op 13 mei 2021).

17 Dit is supervised learning (zie hoofdstuk 5).

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 (TTL)-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 cryptotelefoonoperaties zijn een doorbraak in de opsporing en hebben, naast het live meelezen, geleid tot een enorme hoeveelheid data over de georganiseerde (drugs) criminaliteit die heeft plaatsgevonden. Het gaat dan niet alleen om de teksten uit de tientallen miljoenen berichten, maar ook om foto's die worden meegestuurd en metadata, waaronder locatiegegevens.[18] Om deze data te kunnen benutten, is er tijdens de EncroChat-operatie bij de Dienst Landelijke Recherche (DLR) van de landelijke eenheid een Crypto Analyse Team (CAT) ingericht met zogenaamde sub-CAT's in alle regionale eenheden.[19] Dit heeft zich verder ontwikkeld tot een netwerk van geografische en thematische Crypto Analyse Teams (CAT's) met een Voorziening Crypto Analyseteams (VCAT) bij de landelijke eenheid die de benutting van cryptocommunicatiedata coördineert.[20] In de CAT's worden de cryptocommunicatiedata, onder andere met behulp van geavanceerde software (zie ook hoofdstuk 13), doorzocht. Relevante data kunnen door middel van een proces-verbaal ter beschikking worden gesteld aan lopende opsporingsonderzoeken en worden gebruikt om nieuwe opsporingsonderzoeken te starten. Er zijn – bij iedere dataset (zoals EncroChat) – door de rechter-commissaris voorwaarden gesteld aan het gebruik van de data door de politie, bijvoorbeeld met betrekking tot de trefwoorden die mogen worden gebruikt voor het doorzoeken van de data. Als een bepaalde subset van cryptocommunicatiedata wordt gebruikt voor een (ander) onderzoek, dan moet daarvoor eerst toestemming worden gevraagd aan de rechter-commissaris. In geval van toestemming kunnen de officieren van het opsporingsonderzoek naar de aanbieder (bijvoorbeeld 26Lemont bij EncroChat en 26Argus bij Sky ECC) de informatie delen met de zaaksofficier van het lopende of op te starten opsporingsonderzoek.[21]

De cryptocommunicatiedata hebben de vanzelfsprekende volgorde in de opsporing van georganiseerde (drugs)criminaliteit omgedraaid: van 'zaak zoekt bewijs' naar 'bewijs zoekt zaak'.[22] Voorheen had men – op basis van een signaal – een verdachte in beeld en werd met inzet van allerlei opsporingsmethoden geprobeerd om voldoende

18 Zie bijvoorbeeld https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2022:1274 (voor het laatst geraadpleegd op 13 augustus 2022).

19 Zie onder andere https://www.volkskrant.nl/nieuws-achtergrond/een-reconstructie-van-de-grootste-en-cryptiekraak-ooit-dit-is-voor-de-recherche-puur-genieten (voor het laatst geraadpleegd op 29 juli 2022).

20 Zie hiervoor de derde editie van het magazine *Scherp over intelligencegestuurd politiewerk* (juli 2023) dat wordt uitgegeven vanuit het landelijke programma intelligence van de politie. De thematische CAT's zijn ondergebracht bij de landelijke eenheid. TLL is een voorbeeld van een thematisch CAT.

21 Zie Schermer & Oerlemans 2022. ANOM is een uitzondering, zie noot 5.

22 Zie ook Tops 2022.

bewijsmiddelen voor vervolging te verkrijgen. Nu bevat het verstrekte berichtenverkeer concreet bewijs, maar is de identiteit van de verdachte (veelal) 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)[23] en het analyseren van het geselecteerde berichtenverkeer teneinde er bewijs uit te halen voor het dossier. Er hoeven niet of nauwelijks opsporingsmethoden te worden ingezet om aanvullende gegevens te verzamelen.[24] Opsporingshandelingen worden het sluitstuk, onder andere in de vorm van een aanhouding en doorzoeking.[25] Dit heeft als gevolg dat het recherchewerk (deels) van karakter verandert. Er worden immers dossiers opgesteld zonder dat de verdachte getapt, gevolgd of gezien is.[26] Analyse wint aan belang ten opzichte van 'actie'. Opsporingsonderzoeken duren (mede hierdoor) minder lang.[27] Dit heeft overigens niet alleen maar positieve effecten: door een deel van de rechercheurs worden de zogenaamde 'CAT-zaken' beschouwd als 'administratieve zaken' waar zij minder plezier aan beleven dan aan het 'werken in de actualiteit' (zoals inzet van telefoontaps, opname vertrouwelijke communicatie, observeren en dergelijke).[28]

Het voorgaande maakt dat de cryptocommunicatiedata volgens de politie(leiding) een *gamechanger* in de opsporing zijn. Inmiddels zijn deze data gebruikt in zo'n 1300 opsporingsonderzoeken en de teller loopt door.[29] Hoewel zich rondom de cryptotelefoonoperaties en het gebruik van de verkregen data in strafrechtelijk onderzoek allerlei

23 Voor zover het (sub-)CAT dit nog niet heeft gedaan.

24 Op basis van gesprekken in het kader van lopend empirisch onderzoek kan ik constateren dat zich verschillen voordoen tussen onderzoeksteams. Er zijn onderzoeksteams die de neiging hebben om de beschikbare data te gebruiken als startinformatie – informatie die aanleiding geeft om een opsporingsonderzoek te starten (zie Brinkhoff, 2014) – om vervolgens 'in de actualiteit' te werken met inzet van opsporingsmethoden en primair daarmee bewijs te vergaren. Er zijn ook onderzoeksteams die het dossier zo veel als mogelijk maken op basis van de al beschikbare data en eventueel aanvullend opsporingsmethoden inzetten. Deze keuzes hebben niet alleen te maken met stijlen en voorkeuren (ook van zaaksofficieren), maar vanzelfsprekend ook met de specifieke omstandigheden van het onderzoek.

25 Naarmate de cryptocommunicatiedata meer als startinformatie worden gebruikt, zijn er meer tactische overwegingen aan de orde. In dat geval moet het principe van 'bewijs zoekt zaak' ook worden genuanceerd en is het verschil met de manier van werken van voorheen minder groot.

26 Jansen et al. 2023.

27 De chef van de landelijke recherche geeft daarnaast aan dat politiekorpsen uit andere landen graag 'zakendoen' met de politie in Nederland, omdat zij belang hebben bij de cryptocommunicatiedata en de expertise van de politie in Nederland op dit gebied. Dit maakt dat politiekorpsen in het buitenland eerder geneigd zijn om te voldoen aan verzoeken tot aanhouden en uitleveren van personen die in Nederland worden verdacht van strafbare feiten. Zie https://www.ad.nl/binnenland/het-maakt-niet-meer-uit-in-welk-land-criminelen-zich-schuilhouden-recherche-heeft-sleutelrol-in-de-wereld (voor het laatst geraadpleegd op 14 juli 2023).

28 Zie ook Van Schaik 2022.

29 Jansen et al. 2023.

rechtsvragen voordoen[30], blijkt vooralsnog uit de jurisprudentie dat de cryptocommunicatiedata worden toegelaten als geldig[31] bewijs.[32]. Er zijn inmiddels talloze verdachten (mede) op basis van cryptocommunicatiedata veroordeeld voor zware delicten. Veel kopstukken zitten achter de tralies.[33] Niet alleen kopstukken uit de Nederlandse onderwereld, maar ook hun internationale partners.

De zaak tegen maffiakopstuk Raffaele Imperiale[34]

Op het moment van schrijven – januari 2023 – is er weinig dat de internationale onderwereld meer bezighoudt dan de deal die Raffaele Imperiale heeft gesloten met de Italiaanse overheid. Imperiale wordt beschouwd als één van de belangrijkste maffiabazen van Europa. De cryptocommunicatiedata tonen de verwevenheid tussen Imperiale en Nederlandse criminelen, onder wie Ridouan Taghi en 'Rico de Chileen' (Richard R.). Vanuit de Randstad zijn in de afgelopen jaren grote hoeveelheden cocaïne richting Italië gegaan. Imperiale gebruikte in zowel Nederland als Italië legale ondernemingen, waaronder een groothandel in landbouwproducten uit Westhoek, een koeriersbedrijf op Schiphol en een houtbewerkingsbedrijf uit Haarlem. Hij werd in augustus 2021 aangehouden in Dubai en in maart 2022 uitgeleverd aan Italië. De deal tussen Imperiale en de Italiaanse overheid leidt er naar verwachting toe dat hij uitvoerig gaat verklaren over (zijn partners in) de internationale cocaïnehandel. Het strafdossier van het Italiaanse onderzoek is in belangrijke mate gebaseerd op de cryptocommunicatiedata. 'Het proces-verbaal staat vol met berichten over hoeveelheden, kiloprijzen, aanbieders en afnemers… In de veronderstelling dat alle communicatie afge-

30 Zie hiervoor onder andere: Boeser 2021; Schermer & Oerlemans 2022. Zie ook de brandbrief van oktober 2022 die door 133 strafrechtadvocaten is verstuurd naar onder andere de minister van Justitie & Veiligheid en de Tweede Kamer. Een van de kwesties heeft betrekking op het recht op een eerlijk proces voor verdachten. Dit recht staat volgens sommigen onder druk, onder andere doordat de verdediging beperkt inzicht heeft in het selectieproces dat heeft geleid tot de data die zijn opgenomen in het dossier (zie hiervoor o.a. Te Molder, 2022). Ook voor deze kwestie geldt dat technologie uitkomst kan bieden. Zo kunnen advocaten sinds maart 2023 het platform Hansken gebruiken om de cryptocommunicatiedata in te zien vanaf hun werkplek (zie ook hoofdstuk 13). Zie hiervoor https://www.forensischinstituut.nl/actueel/nieuws/2023/03/20/nfi-maakt-inzage-cryptocommunicatie-op-werkplek-advocaten-mogelijk (voor het laatst geraadpleegd op 26 maart 2023).

31 Dit is overigens nog niet hetzelfde als voldoende (wettig) bewijs. In september 2022 heeft de rechtbank Zeeland-West-Brabant een verdachte van drugshandel vrijgesproken vanwege het ontbreken van wettig bewijs. De verdenkingen waren uitsluitend gebaseerd op Sky ECC-berichten. Bewijsmiddelen moeten volgens de rechtbank afkomstig zijn uit verschillende bronnen of bewijsmiddelen uit één bron moeten worden ondersteund door andere feiten en omstandigheden. Zie: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBZWB:2022:5151 (voor het laatst geraadpleegd op 8 oktober 2022).

32 In dit verband zijn vooral de uitspraken van de Hoge Raad over het gebruik van de Ennetcomdata en de beantwoording van de prejudiciële vragen in EncroChat- en SkyECC-zaken van belang. Zie https://www.hogeraad.nl/actueel/nieuwsoverzicht/2022/juni/hoge-raad-zogenoemde-ennetcomdata-mogen-gebruikt-bewijs/ en https://www.hogeraad.nl/actueel/nieuwsoverzicht/2023/juni/hoge-raad-beantwoordt-prejudiciele-vragen-encrochat-skyecc-zaken/ (beide voor het laatst geraadpleegd op 13 juli 2023). Zie in meer algemene zin ook: Schermer & Oerlemans 2022; Tops 2022.

33 Paulissen 2022.

34 Gebaseerd op https://www.ftm.nl/artikelen/de-nederlands-italiaanse-drugslijn-van-rafaele-imperiale-ontleed (voor het laatst geraadpleegd op 14 juli 2023).

> schermd zou blijven, had de organisatie (van Imperiale, WL) haar drugshandel tot in detail vastgelegd. De betrokkenen voelden zich zo veilig dat ze via hun PGP-telefoons zelfs beelden van hun contrabande deelden', aldus de onderzoeksjournalisten van Follow the Money.

De cryptocommunicatiedata hebben niet alleen een doorslaggevende rol gespeeld in opsporingsonderzoeken naar bekende kopstukken, maar er zijn ook allerlei meer of minder grote sleutelspelers in de georganiseerde drugscriminaliteit bij de politie op de radar gekomen.[35] Het overgrote deel van de enorme hoeveelheid data is echter nog niet benut in opsporingsonderzoek. Er ligt nog voor jaren recherchewerk. De chef van de landelijke recherche is duidelijk: de strafrechtketen piept en kraakt vanwege meer zaken dan capaciteit, maar er komen nog vele zaken aan.[36] Er komen tegelijkertijd nieuwe datasets bij: de operatie met betrekking tot Exclu werd begin februari 2023 naar buiten gebracht.[37] Criminelen stappen over op nieuwe versleutelde manieren van communiceren en de politie zal zich tot het uiterste inspannen om ook deze diensten weer te 'kraken' (zie ook hoofdstuk 7).[38] Exclu zal vermoedelijk niet de laatste zijn.[39]

De cryptocommunicatiedata – en het opsporingsonderzoek dat op basis hiervan wordt uitgevoerd – geven daarnaast een veel beter inzicht in hoe de criminele wereld werkt:[40] de wijze van communicatie, de logistieke processen, de wijze waarop betalingen plaatsvinden, de wijze waarop liquidaties worden aangestuurd,[41] de verschillende rollen die in criminele processen activiteiten uitvoeren, de netwerkstructuren waarin die rollen zijn ingebed, de ambtelijke en niet-ambtelijke corruptie die plaatsvindt, de sleutelplaatsen die worden gebruikt et cetera.[42] Een van de meest verrassende en vernieuwende inzichten heeft betrekking op de criminele geldstromen.[43] Er werd lang vanuit gegaan dat de criminele winsten uit de onderwereld – via allerlei witwasconstructies – in de bovenwereld terechtkwamen. Dit blijkt beperkt te kloppen. Op basis van de cryptocommunicatiedata is het inzicht ontstaan dat het criminele betalingsverkeer de boven-

35 Dit baseer ik op (eigen) lopend empirisch onderzoek.

36 Zie https://www.ad.nl/binnenland/het-maakt-niet-meer-uit-in-welk-land-criminelen-zich-schuilhouden-recherche-heeft-sleutelrol-in-de-wereld (v oor het laatst geraadpleegd op 14 juli 2023).

37 https://www.politie.nl/nieuws/2023/februari/3/politie-leest-opnieuw-mee-met-criminelen.html(voor het laatst geraadpleegd op 4 februari 2023). Exclu werd gebruikt door onder andere de hele top van Satudarah. De cryptocommunicatiedata hebben eraan bijgedragen dat op dit moment vrijwel alle kopstukken van Satudarah zijn opgespoord. Zie https://www.ad.nl/binnenland/het-maakt-niet-meer-uit-in-welk-land-criminelen-zich-schuilhouden-recherche-heeft-sleutelrol-in-de-wereld (voor het laatst geraadpleegd op 14 juli 2023).

38 Bij de landelijke eenheid wordt een nieuw team op het gebied van criminele communicatie opgericht.

39 Zie https://www.ad.nl/binnenland/het-maakt-niet-meer-uit-in-welk-land-criminelen-zich-schuilhouden-recherche-heeft-sleutelrol-in-de-wereld (voor het laatst geraadpleegd op 14 juli 2023).

40 https://www.parool.nl/amsterdam/revolutie-in-de-opsporing-door-miljoenen-gekraakte-chats-het-doel-is-de-criminele-machtsstructuren-echt-af-te-breken (voor het laatst geraadpleegd op 4 februari 2023). Zie ook: Jansen et al. 2023.

41 Van Gestel 2021.

42 https://www.parool.nl/amsterdam/revolutie-in-de-opsporing-door-miljoenen-gekraakte-chats-het-doel-is-de-criminele-machtsstructuren-echt-af-te-breken (voor het laatst geraadpleegd op 4 februari 2023).

43 Zie https://www.ftm.nl/artikelen/ondergronds-bankieren-geldlopers (voor het laatst geraadpleegd op 1 augustus 2023).

wereld bijna niet raakt. De mondiaal opererende criminele netwerken hebben hun eigen, parallelle betalingssysteem waarin het onderling verrekenen – tegen elkaar wegschrijven – van transacties centraal staat, zodat er zo min mogelijk geld in de bovenwereld terecht hoeft te komen.

Kortom: de cryptocommunicatiedata zijn (ook) van grote meerwaarde[44] voor de intelligencepositie van de politie op het gebied van georganiseerde (drugs)criminaliteit.[45] Op basis van een beter beeld van hoe de criminele wereld werkt, kunnen in potentie ook effectievere interventies worden bedacht en uitgevoerd om criminele processen te verstoren. In hoofdstuk 18 wordt hier nader op ingegaan onder de noemer van 'veiligheidsanalyse'.

44 Hierbij moet worden opgemerkt dat het gebruik van de cryptocommunicatiedata ten behoeve van intelligence aan allerlei voorwaarden is verbonden. In de omgeving van het (sub-)CAT kunnen de cryptocommunicatiedata worden gebruikt voor (bredere) analyse, bijvoorbeeld om de accounts van centrale spelers in criminele netwerken te identificeren (en op basis daarvan te prioriteren in de accounts die worden opgepakt). Dergelijke – naar personen herleidbare – analyses kunnen in principe niet buiten het (sub-)CAT worden gedeeld. Dit kan alleen als de analyses niet herleidbaar zijn naar personen, bijvoorbeeld om inzicht te geven in de wijze waarop criminele processen worden uitgevoerd. De cryptocommunicatiedata die in opsporingsonderzoeken zijn gebruikt, kunnen wel worden benut als reguliere opsporingsinformatie.

45 Tops 2022.

13 Digitaal forensisch onderzoek

Digitalisering en dataficatie in de samenleving hebben tot gevolg dat degenen die misdrijven plegen in toenemende mate ook digitale sporen achterlaten.[1] Dit geldt voor alle vormen van criminaliteit waarbij voor digitale criminaliteit geldt dat het hoofdzakelijk digitale sporen betreft.[2] Deze ontwikkelingen maken dat digitaal forensisch onderzoek een steeds grotere rol is gaan spelen in de opsporing.[3] Dit hoofdstuk behandelt het gebruik van technologie bij digitaal forensisch onderzoek.

Potentie van en uitdaging voor digitaal forensisch onderzoek

Digitaal forensisch onderzoek is binnen de forensische wetenschap – het gebruik van wetenschap in het strafrechtelijke systeem – een relatief jong vakgebied.[4] Dit vakgebied heeft betrekking op het herkennen, veiligstellen en analyseren van digitaal opgeslagen gegevens ten behoeve van de strafrechtspleging.[5] Het belang van dit type onderzoek binnen de opsporing is groot, omdat degenen die criminaliteit plegen steeds meer digitale sporen achterlaten.[6] Het gaat dan niet alleen om alle sporen die gebruikers bewust achterlaten door bijvoorbeeld het maken van teksten, foto's en video's, maar ook om de digitale sporen die de huidige besturingssystemen van onder andere smartphones bijhouden.[7] Digitale sporen bevatten vaak informatie over de precieze momenten in de tijd en de precieze volgorde waarin bepaalde activiteiten zijn uitgevoerd.[8] Door relevante gegevensdragers te herkennen en data veilig te stellen, komen deze beschikbaar voor opsporingsonderzoek. Vanaf dat moment kunnen digitale sporen een grote rol spelen bij het beantwoorden van de centrale vragen die in een opsporingsonderzoek aan de orde zijn, waaronder wie betrokken zijn, waar en wanneer een misdrijf is gepleegd en op welke wijze het is gepleegd (zie ook hoofdstuk 26).[9] Neem

1 Henseler & De Poot 2020; Holt, Bossler & Seigfried-Spellar 2022; Zuurveen & Stol 2020.
2 Oerlemans 2020b.
3 Zie ook het rapport van de inspectiedienst in het VK waarin het toenemende belang van digitaal forensisch onderzoek wordt beschreven en tevens wordt geconstateerd dat de politiekorpsen in het VK onvoldoende in staat zijn om de uitdagingen op het gebied van digitaal forensisch onderzoek aan te gaan (HMICFRS, 2022).
4 Holt, Bossler & Seigfried-Spellar 2022; Rogers 2017.
5 Te Molder 2022.
6 Zie ook Jansen et al. 2023.
7 Henseler & De Poot 2020; Meconi & Henseler 2022. Binnen het digitaal forensisch onderzoek is een onderzoeksgebied in opkomst dat dergelijke data onderzoekt om activiteiten te reconstrueren. Dit wordt Pattern-of-Life Forensics (PoLF) genoemd.
8 In dit kader wordt – van oorsprong in het fysiek forensisch onderzoek – ook wel onderscheid gemaakt tussen bewijs op bronniveau (van wie is het spoor) en bewijs op activiteitenniveau (hoe is het spoor ontstaan). Zie Henseler & De Poot 2020.
9 Henseler & De Poot 2020.

als voorbeeld de cryptocommunicatiedata: er zijn talloze opsporingsonderzoeken die op basis van (hoofdzakelijk) deze data zijn afgerond en tot een veroordeling hebben geleid (zie hoofdstuk 12).

Hoewel de beschikbaarheid van digitale sporen kansen biedt voor opsporingsonderzoek, zijn er ook de nodige uitdagingen. Door digitalisering en dataficatie in de samenleving zijn de omvang van en variëteit in de gegevens (data) in opsporingsonderzoeken sterk, zo niet exponentieel, toegenomen.[10] Er is sprake van dubbele groei: er zijn – mede door de opkomst van het IoT – steeds meer gegevensdragers én deze gegevensdragers bevatten steeds meer data.[11] Gegevens komen hierdoor steeds vaker in bulk bij de politie terecht.[12] In een gemiddeld opsporingsonderzoek moet tegenwoordig een enorme hoeveelheid digitale data worden geanalyseerd.[13] Het gaat geregeld om tientallen of zelfs honderden gegevensdragers waarbij iedere drager tientallen of honderden gigabytes aan data kan bevatten (tekstberichten, foto's, video's, gps-locaties, bellijsten et cetera).[14] De groeiende omvang van data is niet alleen zichtbaar in grootschalige onderzoeken die worden uitgevoerd door de regionale recherches en landelijke recherche, maar ook in de opsporingsonderzoeken op districtsniveau en lokaal niveau.[15]

Door deze exponentiële groei zien rechercheurs zich in opsporingsonderzoek voor uiteenlopende uitdagingen gesteld. Hoe vind je in grote hoeveelheden data juist die stukjes data die relevant zijn? Hoe zorg je dat je geen – belastend of ontlastend – bewijs mist? Hoe leg je verbanden tussen verschillende (typen) gegevens? Bij het aangaan van deze uitdaging wordt in toenemende mate gebruikgemaakt van technologie.[16] Niet vanuit luxe, maar vanuit noodzaak.[17] Hierna ga ik in op dit technologiegebruik. Hierbij maak ik een onderscheid tussen digitaal forensische zoekmachines en analysesoftware, al is dit onderscheid in de praktijk niet altijd scherp te maken.

Digitaal forensische zoekmachines

Digitaal forensische zoekmachines worden gebruikt voor het ontsluiten en doorzoeken van omvangrijke datasets.[18] Kenmerkend is dat deze datasets in de regel zo omvangrijk zijn dat deze in praktische zin niet handmatig kunnen worden doorzocht. Bijvoorbeeld:[19] voor een (tactisch) rechercheur zijn honderdduizenden afbeeldingen klaargezet voor onderzoek. Zonder gebruik van technologie is de rechercheur (minimaal) dagenlang door de afbeeldingen aan het scrollen. Als er een nieuwe zoekterm of

10 Mapes 2017; Quick & Raymond Choo 2016; Roest 2021, 2023.
11 Roest 2023.
12 Fedorova et al. 2022.
13 Mapes 2017.
14 Roest 2023.
15 Idem.
16 Ferguson 2017a.
17 Zie Roest 2023.
18 Te Molder 2022.
19 Dit voorbeeld is ontleend aan Roest 2023.

een nieuwe verdachte bijkomt, begint het proces opnieuw. Digitaal forensische zoekmachines zijn bedoeld om de politie tijd en capaciteit te besparen (efficiëntie) en om relevante data te vinden die handmatig wellicht niet gevonden zouden worden. Er kan op hoofdlijnen een onderscheid worden gemaakt tussen twee typen zoekmachines: (vast)geprogrammeerde zoekmachines en machine learning zoekmachines.[20] De geprogrammeerde zoekmachines werken op basis van trefwoorden en hebben als belangrijkste beperkingen dat ze vooral geschikt zijn voor het doorzoeken van tekst en werken op basis van de letterlijke trefwoorden waarmee wordt gezocht. Machine learning zoekmachines zijn ontwikkeld om tegemoet te komen aan de beperkingen van de zoekmachines die op letterlijke trefwoorden werken. Deze zoekmachines kunnen onder andere zoeken op de betekenis van een tekst in plaats van op letterlijke woorden. Dit wordt ook wel semantisch zoeken genoemd en is binnen de politie in ontwikkeling.

Binnen de politie in Nederland wordt al geruime tijd gebruikgemaakt van Hansken. Hansken is een platform met verschillende (typen) digitaal forensische zoekmachines.

Hansken[21]
Hansken is een platform dat vanaf 2015 door het NFI is ontwikkeld.[22] Het platform is vernoemd naar een circusolifant die in de 17de eeuw is geschilderd door Rembrandt.[23] Hansken kon in het publiek van een circusvoorstelling een crimineel aanwijzen. Het doel van platform is om digitale data snel en effectief te doorzoeken en zo bij te dragen aan het opsporen van strafbare feiten. Om in de digitale data te kunnen zoeken, moeten de data – foto's, bezochte internetpagina's, berichtenverkeer, mailverkeer et cetera – worden ingelezen, opgeslagen en geïndexeerd. Hoe meer data, hoe meer tijd dit kost. Hansken kan op dit moment zo'n drie terabyte aan data per uur verwerken, maar is schaalbaar,[24] dus dit neemt na verloop van tijd toe.[25] Als de data beschikbaar zijn, kan de gebruiker snel en efficiënt zoeken met gebruik van uiteenlopende 'tools'. Er kan worden gezocht op alles wat relevant kan zijn, zoals op woorden[26] en eigenschappen van sporen (bijvoorbeeld alleen mails of foto's). De gebruiker kan de zoekresultaten blijven filteren totdat er uit miljoenen sporen een selectie is gemaakt. De bestanden van de gemaak-

20 Zie ook Te Molder 2022, die overigens een iets ander onderscheid maakt.
21 Deze tekst is gebaseerd op verschillende bronnen. Zie voor algemene informatie: https://www.forensischinstituut.nl/forensisch-onderzoek/hansken (voor het laatst geraadpleegd op 13 mei 2021). Zie voor een voorbeeld van het gebruik: Hirsch Ballin & Oerlemans 2023.
22 Het betreft een doorontwikkeling van het eerdere systeem Xiraf, dat (gezien de toenemende hoeveelheid data) onvoldoende schaalbaar was.
23 Zie hiervoor https://www.agconnect.nl/artikel/superscience-digital-forensics-om-scenarios-te-testen (voor het laatst geraadpleegd op 28 juli 2022).
24 Het platform is gebaseerd op Hadoop; een open source framework voor big data.
25 Bas Seyyar & Geradts 2020.
26 Het zoeken op woorden kent overigens wel beperkingen, omdat je veelal veel niet relevante hits krijgt en het risico loopt dat de data die je zoekt niet worden gevonden, omdat het woord niet letterlijk in de data voorkomt (in geval van tekst). Zie ook het eerder gemaakte onderscheid tussen de twee typen zoekmachines.

te selectie zijn één voor één te bekijken. De geselecteerde data kunnen worden weergegeven op een tijdlijn, bijvoorbeeld in geval van e-mailverkeer of chatgesprekken. Het is ook mogelijk om netwerken van apparaten in kaart te brengen die zijn gekoppeld aan personen. Hansken wordt in Nederland gebruikt door steeds meer opsporingsdiensten, waaronder de politie. Het platform is inmiddels gebruikt in meer dan duizend strafzaken.[27] Ook internationaal is er veel interesse.[28]

Hansken is een platform waarop verschillende applicaties worden ontwikkeld.[29] Dit betreft in toenemende mate machine learning zoekmachines voor het meer geavanceerd doorzoeken van digitale data.[30] Een voorbeeld hiervan is FIRE: forensic image recognition engine.[31] FIRE is een machine learning algoritme voor forensisch fotomateriaal. De aanleiding voor FIRE ontstond enkele jaren geleden in een drugsonderzoek waarin rechercheurs honderdduizenden foto's moesten doorspitten op zoek naar specifieke zeecontainers. Monnikenwerk dat volgens de datawetenschappers van het NFI gemakkelijker moest kunnen. Op basis van bestaande modellen hebben zij een zelflerend algoritme ontwikkeld (getraind) dat in staat is om een speld in een hooiberg te vinden. Dit algoritme kan zeecontainers, bankpassen, vuurwapens, wiet en harddrugs herkennen, evenals teksten op afbeeldingen (zoals persoonsgegevens op rijbewijzen). Rechercheurs kunnen nu in een dataset zoeken naar een bepaalde categorie afbeeldingen. De datawetenschappers van het NFI zijn vooral bezig met het verzamelen van data om het algoritme te trainen, onder andere ten behoeve van het herkennen van een nieuwe objecten op afbeeldingen.

Naast Hansken worden er binnen de politie uiteenlopende (andere) tools gebruikt om allerlei digitale data effectief en efficiënt te doorzoeken, zoals teksten, foto's, video's en spraakberichten. Deze tools worden onder andere ontwikkeld door het Team Rendement Operationele Informatie (TROI). Dit team is enkele jaren geleden in de politie-eenheid Amsterdam ontstaan en heeft als missie om operationele (big) data inzichtelijk te maken voor uitvoerende politiemensen, in het bijzonder voor (tactisch) rechercheurs.[32] De bedoeling van TROI is dat rechercheurs of andere uitvoerende

27 Hirsch Ballin & Oerlemans 2023.
28 https://www.forensischinstituut.nl/actueel/nieuws/2020/06/22/opsporingsdiensten-ontwikkelen-hansken-samen-verder (voor het laatst geraadpleegd op 13 mei 2021).
29 Het platform beschikt ook over diensten waarmee gebruikers zelf programma's kunnen schrijven, zoals Hansken.py en de Hansken Extraction Plugin.
30 Zie Mapes 2017. Zie ook https://thenextweb.com/news/how-to-build-a-search-engine-for-criminal-data (voor het laatst geraadpleegd op 13 mei 2021).
31 https://magazines.forensischinstituut.nl/atnfi/2021/35/duizenden-fotos-sneller-doorzoeken-dankzij-slim-algoritme (voor het laatst geraadpleegd op 13 mei 2021)
32 Roest 2021, 2023.

politiemensen zelf met de data werken.[33] Ten behoeve hiervan worden door TROI tools ontwikkeld die in de regel gebruikmaken van AI, waaronder opensource-algoritmen voor beeld- en spraakherkenning.[34] Deze algoritmen worden specifiek getraind voor de taken van de politie. Naast specifieke zoekmachines is er door TROI een triagetool ontwikkeld die binnen een opsporingsonderzoek verschillende digitale gegevensdragers kan prioriteren en kan aangeven welke aanknopingspunten er per geprioriteerde gegevensdrager zijn.[35] De data vanuit verschillende gegevensdragers worden hierbij doorzocht op basis van een thema en indicatorenlijst. TROI-pionier van het eerste uur – Dominique Roest – licht de hoofdlijnen van deze applicatie toe:

> *'In een groot aantal onderzoeken naar witwassen, zijn tientallen telefoons in beslag genomen. Normaal gesproken spitten collega's deze telefoons handmatig door, op zoek naar signalen die wijzen op (onverklaarbaar) vermogen. Een tijdsintensief proces, waarbij er waarschijnlijk signalen over het hoofd worden gezien. Samen met analisten en rechercheurs heeft TROI geautomatiseerde zoekopdrachten opgesteld. Daarna werd het vinden van bitcoinwallets, auto's, boten en chats over grote geldbedragen een kwestie van één druk op de knop. Een mooi voorbeeld van kunstmatige intelligentie in de praktijk.'*[36]

Naast tools om data te (door)zoeken werkt TROI ook aan andere toepassingen die voor het politiewerk van meerwaarde kunnen zijn, zoals modellen om *deepfakes* te herkennen.[37] Gegeven de verwachte groei in het aantal deepfakes dat in de samenleving 'terechtkomt' – zie hoofdstuk 9 – is het herkennen van deepfakes een opgave die in de komende jaren van belang is. TROI is een voorbeeld van een innovatieteam of -netwerk dat zich in de afgelopen jaren heeft uitgebreid naar meer eenheden van de politie (zie ook hoofdstuk 23).[38] Een ander voorbeeld van een innovatieomgeving binnen de politie is het Q-LAB dat in diverse eenheden is ingericht als begeleider van het innovatieproces. Ook vanuit deze Q-LAB's wordt er (soms) gewerkt aan het ontwikkelen van tools in het kader van digitaal forensisch onderzoek. Zo experimenteert het Q-LAB van de politie in Oost-Nederland met het gebruik van voice-ID: een AI-toepassing voor identificatie van personen op basis van biometrisch stemgeluid.[39] Voice-ID

33 De lokale teams van TROI hebben op hoofdlijnen twee functionaliteiten ingericht: zaakondersteuning en development. Zaakondersteuning ontwikkelt binnen een opsporingsonderzoek kleine programma's om de data voor het betreffende onderzoek beter te kunnen benutten. Development gaat aan de slag met de vragen die in veel meer opsporingsonderzoeken spelen (of meer het karakter van een intelligencevraag hebben). De appstore van TROI bestaat inmiddels uit dertien tools. Zie hiervoor de derde editie van het magazine *Scherp over intelligencegestuurd politiewerk* (juli 2023).

34 Zie bijvoorbeeld https://tweakers.net/plan/2800/crimediggers-van-de-politie-zijn-altijd-op-zoek-naar-data-en-verbanden.html (voor het laatst geraadpleegd op 9 oktober 2022).

35 Roest 2023.

36 Roest 2021: 15.

37 https://it.kombijdepolitie.nl/patronen-ontdekken (voor het laatst geraadpleegd op 9 oktober 2022).

38 Zie het eerdergenoemde *magazine Scherp op intelligencegestuurd politiewerk*.

39 Ik baseer me hierbij op uitgebreide berichtgeving op LinkedIn over dit experiment. Medio 2023 is er een basisversie (minimal viable product) opgeleverd. Er wordt gewerkt aan landelijke inzetbaarheid.

kan binnen de opsporing (onder andere) worden gebruikt om stemgeluiden – die worden opgenomen via bijvoorbeeld tapgesprekken of de opname van vertrouwelijke communicatie (OVC) – met elkaar te vergelijken. Zo kun je vaststellen of de persoon die in tapgesprek X dezelfde persoon is als in tapgesprek Y of in een opname op een locatie.
Onderzoek naar en ontwikkeling van software voor digitaal forensisch onderzoek vinden ook plaats bij hogescholen en universiteiten, vaak in samenwerking met het NFI. Zo wordt er door onder andere door het lectoraat *Digital Forensics & E-Discovery* van de Hogeschool Leiden onderzoek gedaan naar de mogelijkheden van het gebruik van ChatGPT in digitaal forensisch onderzoek.[40] Een ander voorbeeld is AI4forensics.[41] Dit is een onderzoekslab van het NFI en de Universiteit van Amsterdam gericht op het doen van (promotie)onderzoek naar het gebruik van AI in forensisch onderzoek. Dit lab is begin 2023 geopend vanuit de verwachting dat AI het forensisch onderzoeksveld in de komende jaren ingrijpend gaat veranderen. Er wordt onderzoek gedaan naar onder andere sprekersherkenning, het herkennen van deepfakes,[42] het herkennen van verborgen berichten in foto's of video's (zie hoofdstuk 7) en het herkennen van witwaspatronen.

Al deze voorbeelden maken duidelijk dat er binnen en rondom de politie in Nederland de nodige ontwikkelingen plaatsvinden gericht op verbetering van het opsporingswerk door gebruik van technologie. De volgende paragraaf gaat hier verder op in door aandacht te besteden aan analysetechnologie.

Geavanceerde analysesoftware
Een bruikbare metafoor voor het recherchewerk is puzzelen. Door middel van opsporingsmethoden worden puzzelstukjes – stukjes data – verzameld en hiermee wordt een puzzel gelegd:[43] '… piecing together fragments of information', aldus Matthew Bacon.[44] In opsporingsonderzoek moeten er verbanden tussen stukjes data worden gelegd. Welke data je nodig hebt en welke verbanden er zijn, is op voorhand niet te zeggen. Opkomende technologieën kunnen de politie ondersteunen bij het identificeren van patronen, leggen van verbanden (binnen en tussen opsporingsonderzoeken) en het visualiseren van deze verbanden. De politie in Nederland benut deze mogelijkheden en maakt sinds enkele jaren gebruik van een voorziening die de Raffinaderij wordt genoemd.

40 Henseler & Van Beek 2023. Zie ook de publicatie van Cognyte: https://engage.cognyte.com/s/ad2e4911/chatgpt-law-enforcement-report (voor het laatst geraadpleegd op 16 juli 2023).
41 https://www.forensischinstituut.nl/actueel/nieuws/2023/03/13/uva-en-nfi-openen-forensisch-onderzoekslab-ai4forensics (voor het laatst geraadpleegd op 14 maart 2023).
42 https://www.forensischinstituut.nl/actueel/nieuws/2022/11/15/nieuwe-methodes-nfi-en-uva-voor-herkennen-deepfakes (voor het laatst geraadpleegd op 4 januari 2023).
43 Landman, Kouwenhoven & Brussen 2020.
44 Bacon 2016: 7.

Raffinaderij[45]

In 2011 werd de politie in het onderzoek naar het netwerk van Robert M., de hoofdverdachte in de omvangrijke kinderpornozaak uit Amsterdam, geconfronteerd met grote hoeveelheden (digitale) data die moesten worden geanalyseerd.[46] Er was behoefte aan een werkwijze en ondersteunende (IT)-voorzieningen om rechercheurs en analisten in staat te stellen om grote hoeveelheden data op een intelligente manier te ontsluiten en te analyseren. Dat was de aanleiding om een proeftuin te starten met als doel om op basis van de informatiebehoefte van de verschillende betrokkenen (OM, rechercheur, analist) een passende voorziening te ontwikkelen. Dit heeft geresulteerd in de Raffinaderij: een voorziening om snel grote hoeveelheden politiegegevens in samenhang met elkaar te analyseren en te visualiseren. Zo kunnen data afkomstig van in beslag genomen telefoons en computers in samenhang met alle andere relevante onderzoeksdata – bijvoorbeeld uit de basisinformatiesystemen, telefoontaps, bakens, internetdata, gegevens van ANPR – worden ontsloten en geanalyseerd. Hierdoor kunnen verbanden worden ontdekt tussen schijnbaar niet-gerelateerde gebeurtenissen of kunnen veronderstelde verbanden juist in een vroeg stadium worden ontkracht. Vandaar de naam 'Raffinaderij': ruwe data worden opgewerkt tot verschillende bruikbare informatieproducten. Het is een proces van 'raffineren'. Met betrekking tot het gebruik van gegevens geldt dat het moet gaan om gegevens die rechtmatig in een opsporingsonderzoek zijn gebracht en die worden verwerkt met een duidelijke doelbinding (zie ook hoofdstuk 27). De werkwijze van de Raffinaderij is in het bijzonder – maar zeker niet alleen – bruikbaar bij titel V-onderzoeken naar de georganiseerde misdaad en titel VB-onderzoeken naar terrorisme.[47]

De Raffinaderij maakt gebruik van software van Palantir, een bedrijf uit Silicon Valley in de VS.[48] Het platform van Palantir wordt door politiekorpsen in de VS gebruikt,[49] maar ook door de politie in Duitsland (hessenDATA)[50] en Denemarken (POL-INTEL systeem).[51] De kracht van dit platform is gelegen in het leggen en visualiseren van verbanden op basis van grote hoeveelheden, diverse data uit uiteenlopende bronnen.

45 De Vries 2017.
46 De 'Amsterdamse zedenzaak' is ook de aanleiding geweest voor het ontstaan van het eerder behandelde TROI.
47 Zie Van den Eeden et al. 2021.
48 Ik baseer me hierbij vooral op een informatieverzoek dat op basis van de Wet openbaarheid van bestuur (Wob) is ingediend door – naar ik vermoed – Bits of Freedom, een Nederlandse stichting voor digitale burgerrechten. Zie https://www.politie.nl/binaries/content/assets/politie/wet-open-overheid/11-landelijke-eenheid/overige-documenten/2021/palantir/20210317---8256---besluit-met-bijlage_def-.pdf . Zie ook Schuilenburg & Soudijn (2021) die Palantir noemen als een van de big data-toepassingen waarvan de politie in Nederland gebruikmaakt.
49 Brayne 2021.
50 Egbert & Leese 2021.
51 Zie https://edri.org/our-work/new-legal-framework-for-predictive-policing-in-denmark/ (voor het laatst geraadpleegd op 8 oktober 2022).

Het platform van Palantir structureert de (deels) ongestructureerde data uit verschillende bronnen en maakt zo het geautomatiseerd analyseren van deze data mogelijk. Met behulp van de software kan bijvoorbeeld inzicht worden verkregen in de locaties waar bepaalde personen wanneer zijn geweest; er ontstaat min of meer automatisch een tijdlijn van de periode rondom het moment waarop het delict is gepleegd. De software van Palantir kan – op basis van de adresboeken uit mobiele telefoons – tevens een netwerkschema van contacten maken: wie zijn aan elkaar gerelateerd?[52] Dit soort analyses bespaart rechercheurs of analisten (heel) veel tijd. Sarah Brayne deed onderzoek naar (onder andere) het gebruik van Palantir bij het *Los Angeles Police Department* (LAPD) en formuleert de meerwaarde van het platform als volgt:

> *'Data – particularly large, diverse sets of data – are relatively useless on their own. You need a good platform. And Palantir is excellent at processing, sorting, and analyzing data. With the right platform, searches that used to take hours, days, or even weeks may now only take a few seconds.'*[53]

De verwachting is dat de politie met een voorziening als de Raffinaderij veel meer uit de beschikbare data kan halen en tevens haar handelingssnelheid verhoogt. De Raffinaderij heeft in verschillende opsporingsonderzoeken inmiddels haar meerwaarde laten zien.[54] Een voorbeeld is het omvangrijke 26Koper-onderzoek naar aanleiding van de vele liquidaties in de onderwereld.[55] Met behulp van de geavanceerde analyses van de Raffinaderij zijn relaties gelegd tussen meerdere zaken en is men op het spoor gekomen van de zogenaamde Utrechtse liquidatiegroep. En zo zijn er meer voorbeelden. Klerks en Vink-Teeven merken het volgende op:

> *'Raffinaderij, de voorziening die gegevens uit tientallen opsporingsonderzoeken tegelijk kan extraheren en grafisch kan presenteren, betekent niets meer dan een doorbraak. Onderzoeken met grote hoeveelheden data zoals naar liquidaties en motorbendes zouden veel lastiger of zelfs niet uit te voeren zijn zonder dergelijke data analyse technologieën.'*[56]

Het voorgaande maakt vooral duidelijk hoe digitalisering in de opsporing een tweesnijdend zwaard is: het zorgt voor groeiende hoeveelheden data in opsporingsonderzoeken en helpt tegelijkertijd om die groeiende hoeveelheden data hanteerbaar te ma-

52 Bij dit type analyses is alertheid nodig op het opnemen en analyseren van data van onverdachte personen. In verband hiermee heeft de politie in de deelstaat Hamburg in Duitsland van de rechter restricties opgelegd gekregen bij het gebruik van de software van Palantir (hessenDATA). Zie https://www.wired.com/story/palantir-germany-gotham-dragnet/ (voor het laatst geraadpleegd op 21 februari 2023). Zie ook hoofdstuk 27 over bulkdatasets en privacy.

53 Brayne 2021: 40.

54 De betreffende software van Palantir kan overigens ook van meerwaarde zijn bij veiligheidsanalyse (zie hoofdstuk 18) en wordt (in ieder geval) in andere landen ook hiervoor gebruikt.

55 De Vries 2017.

56 Klerks & Vink-Teeven 2020: 170.

ken. Het is te verwachten dat er in de komende jaren nog vele innovaties op dit gebied gaan plaatsvinden, die zowel de effectiviteit als efficiëntie[57] van de opsporing kunnen gaan verbeteren (zie ook hoofdstuk 26).

57 Zo is de politie al jaren bezig met het ontwikkelen van automatische spraakherkenning ten behoeve van het politiewerk (zie Schuilenburg & Soudijn, 2021). Spraaktechnologie kan een rol spelen bij het omzetten van video en/of audio naar tekst ten behoeve van processen-verbaal. Dit kan in het opsporingsproces in potentie veel tijdwinst opleveren.

14 Slimme camera's

Aan het einde van de jaren negentig van de vorige eeuw heeft cameratoezicht in Nederland zijn intrede gedaan en sinds die tijd is het aantal camera's in het publieke domein fors toegenomen.[1] Door gebruik te maken van *closed-circuit television* (CCTV)-camera's werd het mogelijk om op afstand waar te nemen.[2] Deze camera's registreren de stroom van gebeurtenissen in een bepaald gebied, maar bevatten geen intelligentie. Sinds 2004 wordt er ook gebruikgemaakt van camera's met (meer) intelligentie. Dit zijn camera's met *computer vision technology* (zie hoofdstuk 5).[3] Met deze technologie kunnen camera's met behulp van algoritmen automatisch bepaalde fenomenen herkennen en signaleren/alerteren. Hierna ga ik in op verschillende typen slimme camera's.

Camera's die kentekens herkennen

Het gebruik van slimme camera's door de politie in Nederland is gestart met ANPR-camera's. ANPR staat voor *automatic number plate recognition*: het betreft dus een camera die automatisch een kenteken kan herkennen.[4] ANPR-camera's werken op basis van algoritmen die een beeld omzetten in een gelezen kenteken. ANPR-camera's kunnen in beginsel op twee manieren worden gebruikt.[5]

De eerste manier is de oorspronkelijke manier, die al ruim vijftien jaar wordt gebruikt: ingelezen kentekens worden vergeleken met kentekens op referentielijsten en alleen die kentekens worden vastgelegd.[6] Referentielijsten bevatten kentekens van auto's die worden gezocht door de politie, bijvoorbeeld omdat een auto is gestolen, iemand voortvluchtig is of een boete heeft openstaan. Er zijn verschillende referentielijsten in

1 Zie https://nl.wikipedia.org/wiki/Cameratoezicht (voor het laatst geraadpleegd op 7 oktober 2022). Er hangen ruim tweehonderdduizend camera's in de openbare ruimte. Daarnaast heeft een groot aantal bedrijven en particulieren een eigen bewakingscamera. Het gaat op dit moment naar schatting om zo'n anderhalf miljoen camera's. De politie heeft interesse in deze digitale ogen en vraagt sinds 2016 aan bedrijven en particulieren om hun camera vrijwillig aan te melden bij de politie. De locatie en andere gegevens van de camera(eigenaar) worden opgenomen in de database 'camera in beeld', die enkele jaren geleden ongeveer driehonderdduizend camera's bevatte. Met deze database kan de politie nog sneller zien waar in de buurt van een gepleegd misdrijf camera's zijn die mogelijk beelden van de dader hebben geregistreerd.

2 Zie Newburn & Hayman 2002.

3 Skogan 2019.

4 De technologie voor ANPR-toezicht is in de jaren zeventig in het VK ontwikkeld, mede om het hoofd te bieden aan de dreiging van terroristische aanslagen door de IRA in London (zie Homburg et al. 2016).

5 Zie hoofdstuk 17 voor het gebruik van ANPR-camera's in het kader van het identificeren van verdacht gedrag.

6 Van Berkel, Van den Eeden & De Poot 2020.

gebruik; het zijn er inmiddels in ieder geval zo'n tweehonderd.[7] Hierbij kan worden gedacht aan een lijst met gesloten auto's, een lijst met auto's die worden gebruikt voor mobiel banditisme, maar ook lijsten die zijn gekoppeld aan specifieke opsporingsonderzoeken. Daarnaast kunnen er bij incidenten kentekens worden ingevoerd, zoals gebeurde bij de moord op Peter R. de Vries (zie ook hoofdstuk 17). Uit evaluatieonderzoek komt naar voren dat uitvoerende politiefunctionarissen positief zijn over de bijdrage die dit gebruik van de ANPR-camera levert aan het dagelijks politiewerk, in het bijzonder waar het gaat om het opsporen van gestolen voertuigen, opsporen van specifieke personen, tegengaan van mobiel banditisme en het innen van boetes.[8]

De tweede manier is sinds 2019 in gebruik: ingelezen kentekens worden vastgelegd ten behoeve van eventuele opsporing. Dit wil zeggen dat alle passerende en geregistreerde kentekens worden opgeslagen in een database (Argus). Deze database kan worden bevraagd in verband met opsporingsonderzoek. Het opslaan (vastleggen) van kentekens vindt plaats op basis artikel 126jj van het Wetboek van Strafvordering (Sv).[9] Bijvoorbeeld: als er ergens een overval is gepleegd, kan de politie – op bevel van een officier van justitie – alle kentekens opvragen van voertuigen die rond de tijd van de overval door een ANPR-camera in de buurt zijn geregistreerd.[10] Als er een kenteken tussen zit dat op naam staat van iemand die al eerder betrokken is geweest bij een overval, dan kan de politie dit gebruiken als aanknopingspunt voor het recherchewerk. Met alleen referentielijsten is dit niet mogelijk, omdat – vanuit het uitgangspunt van dataminimalisatie (zie hoofdstuk 27) – alleen de kentekens worden opgeslagen die op referentielijsten voorkomen. Uit evaluatieonderzoek komt naar voren dat bewaarde kentekens vooralsnog vooral zijn gebruikt ten behoeve van sturingsinformatie in opsporingsonderzoeken: het is dan een 'plusje' om verder richting te geven aan het onderzoek.[11] Of anders gezegd: het wordt gebruikt in combinatie met andere opsporingsmiddelen.

Het aantal ANPR-camera's heeft zich vanaf 2004 bij voortduring uitgebreid.[12] Op dit moment heeft de politie ongeveer driehonderd vaste ANPR-camera's in beheer.[13] Daarnaast zijn er ongeveer honderdvijftig politievoertuigen uitgerust met een ANPR-camera's (mobiele ANPR-camera's). Het is onbekend hoeveel flexibele ANPR-ca-

7 https://www.nrc.nl/nieuws/2021/08/30/even-kijken-wie-de-chauffeur-is-handig-toch (voor het laatst geraadpleegd op 30 december 2021).
8 Bantema et al. 2018.
9 Het is hierbij van belang dat alleen het kenteken wordt vastgelegd. Een deel van deze camera's heeft in het verleden ook foto's van bestuurder en eventuele bijrijder vastgelegd, maar er was geen juridische grondslag om personen herkenbaar in beeld te brengen. Om die reden kwam in oktober 2022 het bericht naar buiten dat de politie de voorruit op de foto's automatisch gaat blinderen of 'blurren'. Zie: https://www.politie.nl/nieuws/2022/oktober/24/voorruiten-anpr-fotos-automatisch-geblindeerd.html (voor het laatst geraadpleegd op 3 januari 2023).
10 Zie ook https://www.nrc.nl/nieuws/2021/08/30/even-kijken-wie-de-chauffeur-is-handig-toch (voor het laatst geraadpleegd op 30 december 2021).
11 Van Berkel, van Uden & De Poot 2021.
12 Zie bijvoorbeeld https://www.nrc.nl/nieuws/2017/11/12/politie-installeert-200-nieuwe-kentekencameras (voor het laatst geraadpleegd op 30 december 2021).
13 Deze alinea is in belangrijke mate gebaseerd op van Berkel et al. 2020.

mera's de politie in beheer heeft. De politie heeft daarnaast toegang tot ANPR-camera's van anderen, zoals die van de Koninklijke Marechaussee. In totaal heeft de politie vandaag de dag de beschikking over zo'n zestienhonderd ANPR-camera's. Ruim dertienhonderd hiervan zijn aangewezen als camera's om kentekengegevens van passerende voertuigen te registreren en op te slaan voor een periode van 28 dagen. Deze dertienhonderd camera's registreren gemiddeld zo'n 4,3 miljoen passages per dag waarvan ongeveer de helft een uniek kenteken heeft.

Camera's die bepaalde gedragingen herkennen
Een ANPR-camera zet een beeld om in een kenteken. Dit is een relatief eenvoudige vorm van CVT. Een meer actuele innovatie betreft slimme camera's die bepaalde gedragingen herkennen. Dergelijke camera's worden net zo lang getraind met data totdat zij in staat zijn om op basis van videobeelden bepaald gedrag te identificeren. In het kader van politiewerk gaat het dan in de eerste plaats om gedragingen die zijn verboden en als zodanig zijn vastgelegd in wetgeving. In Nederland hebben de eerste camera's met deze vorm van intelligentie hun intrede gedaan.

MONOcam: slimme camera voor verkeershandhaving[14]
In juli 2021 bracht de politie het bericht naar buiten dat zij slimme camera's gaat inzetten tegen afleiding in het verkeer (bestuurders die een apparaat – mobiele telefoon – in handen hebben); een van de grootste veroorzakers van verkeersongelukken. De slimme camera heet de MONOcam en is grotendeels door de politie zelf ontwikkeld. De software is gedurende anderhalf jaar 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 verstuurt. Alle politie-eenheden krijgen deze slimme camera's. Met deze camera's moet het aantal ongelukken door afleiding in het verkeer worden teruggebracht. Nederland is het eerste Europese land dat deze technologie gebruikt. In Australië wordt er al enige tijd met succes mee gewerkt. De Autoriteit Persoonsgegevens (AP) heeft het proces goedgekeurd, wat wil zeggen dat het gebruik van de MONOcam voldoet aan de wet- en regelgeving op het gebied van

14 Gebaseerd op https://www.politie.nl/nieuws/2021/juli/1/00-monocam-ingezet-tegen-afleiding-in-verkeer.html (voor het laatst geraadpleegd op 7 oktober 2020). Zie ook https://nos.nl/artikel/2481555-nieuwe-slimme-camera-s-aangeschaft-om-appende-bestuurders-te-betrappen (voor het laatst geraadpleegd op 16 juli 2023).

privacy (zo worden gezichten van medepassagiers geblindeerd en worden de foto's verwijderd wanneer deze zijn doorgestuurd naar het CJIB). Volgens het OM leidt het gebruik van de camera's tot een pakkans van 95%. In juli 2023 werd door de politie en het OM naar buiten gebracht dat de politie een toenemend aantal MONOcams heeft aangeschaft. De slimme camera's worden tevens op vaste plekken opgehangen (de oorspronkelijke MONOcam is een mobiele camera).

Het is waarschijnlijk dat de ontwikkeling en het gebruik van algoritmen voor het herkennen van overtredingen, misdrijven en ordeverstoringen gaan toenemen.[15] Naast het herkennen van overtredingen en misdrijven worden slimme camera's ook gebruikt voor verdacht gedrag of verdachte situaties. Hierbij wordt gebruikgemaakt van een profiel en van meerdere databronnen om te bepalen of het profiel zich in de praktijk voordoet. Deze technologie omvat (veelal) meer dan een slimme camera, al is een slimme camera er wel een onderdeel van. Het taxeren van verdacht gedrag of verdachte situaties wordt behandeld in hoofdstuk 17.

Camera's die gezichten herkennen

Het laatste type slimme camera[16] is in staat tot gezichtsherkenning. Gezichtsherkenning is een biometrische techniek[17] die kan worden gebruikt om personen te identificeren.[18] De technologie werkt op basis van biometrische beschrijvingen van gezichten, ook wel gezichtstemplates genoemd. Een dergelijke template is een rij van getallen (het is een digitale template).[19] Gezichtsherkenning vindt plaats doordat software de template van een – op de een of andere manier (foto, videobeeld) – opgenomen persoon vergelijkt met templates die zijn opgeslagen in een database. Om die reden wordt de term 'gelaatsvergelijking' ook weleens gebruikt.

15 Dit vindt overigens niet alleen plaats door of in opdracht van de politie en/of het OM. De gemeente Den Haag heeft – samen met partners – in het Living Lab Scheveningen (zie hoofdstuk 20) een succesvolle proef gedaan met het gebruik van een slimme camera voor detectie van (gebruik van) lachgas. Zie hiervoor: https://www.binnenlandsbestuur.nl/digitaal/den-haag-positief-over-test-met-lachgasdetectie (voor het laatst geraadpleegd op 16 juli 2023).

16 Voor zover hier behandeld. Er zijn meer type slimme camera's, maar die zijn vooralsnog voor Nederland minder relevant. Zo zijn er in de VS camera's met gunshot detection technology (GDT); aan deze camera's zijn akoestische audiosensoren toegevoegd. Zie Skogan (2019). De politie in Nederland heeft zich ook op deze technologie georiënteerd.

17 Biometrie gaat over het verzamelen en verwerken van iemands unieke lichaams- of gedragskenmerken, vaak met het doel om die persoon te identificeren of de identiteit te controleren (zie Gerritsen et al. 2020). DNA-onderzoek (zie hoofdstuk 11) en stemidentificatie (zie hoofdstuk 13) zijn ook biometrische technieken.

18 In de context van politiewerk gaat het dan om personen die er geen belang bij hebben om mee te werken aan gezichtsherkenning. Dit wordt ook wel niet-coöperatieve gezichtsherkenning genoemd en moet worden onderscheiden van gezichtsherkenning waaraan een persoon meewerkt, bijvoorbeeld bij het ontgrendelen van de smartphone. Zie verder: Van Rest et al. 2021.

19 Van Rest et al. (2021) merken op dat er geen internationale standaard is voor gezichtstemplates.

Er kan *op hoofdlijnen* onderscheid worden gemaakt tussen twee vormen van gezichtsherkenning: *face identification* en *face surveillance.* [20] Face identification wil zeggen dat er 'achteraf' een poging tot identificatie van een persoon wordt uitgevoerd door een template te vergelijken met templates in een database. Dit is een opsporingsmiddel. Deze manier van gezichtsherkenning is de enige manier waarop gezichtsherkenning op dit moment door de politie in Nederland plaatsvindt.

CATCH[21]

Sinds omstreeks 2017 wordt er door de politie in Nederland gebruikgemaakt van geavanceerde gezichtsherkenningssoftware. Deze software wordt CATCH genoemd: Centrale Automatische TeChnologie voor Herkenning van personen. CATCH is bedoeld om verdachten op te sporen. De software wordt gebruikt door een afdeling van de landelijke eenheid die is gespecialiseerd in gezichtsherkenning (Centrum voor Biometrie). De afdeling krijgt van tactische opsporingsteams foto's van *verdachten* met de vraag om deze te identificeren (er is ook een app beschikbaar waarmee politieagenten foto's en beelden naar CATCH kunnen sturen). Deze foto's komen uit diverse bronnen, zoals beveiligingscamera's, foto's van observatie-eenheden, bodycams en sociale media. Nadat de foto is beoordeeld op kwaliteit wordt deze door de software vergeleken met foto's van meer dan 1,3 miljoen veroordeelden en arrestanten die zijn opgenomen in een (groeiende) database.[22] Op basis van de vergelijking vindt er al dan niet een match plaats (met één of soms meer personen). De match wordt door twee biometrische experts onafhankelijk van elkaar beoordeeld. Als de match van de computer wordt bevestigd, dan wordt dit beschouwd als een *indicatie* van iemands identiteit. De software analyseert een foto op basis van algoritmen. De ervaringen wijzen vooralsnog uit dat de software behoorlijk nauwkeurig is. Ook foto's met een bedekt gezicht of een petje leiden veelal tot positieve resultaten. Bij twijfelgevallen krijgt een tactisch opsporingsteam veelal foto's van meerdere personen met de boodschap dat deze personen op de verdachte lijken. Er

20 Zie Ferguson (2020a) voor een uitgebreide behandeling van gezichtsherkenning ten behoeve van politiewerk.

21 Deze inhoud is vooral gebaseerd op https://www.nrc.nl/nieuws/2018/02/19/politiesoftware-scant-gezichten-van-verdachten en https://www.nu.nl/tech/6025903/onduidelijk-hoe-vaak-gezichtsherkenning-bij-politie-leidt-tot-aanhoudingen.html (beide voor het laatst geraadpleegd op 16 januari 2020). Daarnaast is berichtgeving gebruikt uit 2021: https://www.nu.nl/tech/6121460/tienduizenden-mensen-mogelijk-onterecht-in-gezichtendatabase-van-de-politie.html en https://www.nu.nl/tech-achtergrond/6121506/de-impact-van-gezichtsherkenning-een-gezicht-als-bewijs-voor-criminaliteit.html (beide voor het laatst geraadpleegd op 2 augustus 2021).

22 Naast deze database is er ook een database met 8 miljoen gezichtsfoto's van zeker 6,5 miljoen personen die in de vreemdelingenadministratie zijn geregistreerd. Hierin staan o.a. expats, asielzoekers en buitenlandse studenten die van buiten de EU naar Nederland komen. In februari 2023 kwam dit – naar aanleiding van onderzoek van *RTL Nieuws* – in de media waarbij de suggestie werd gewekt dat dit onwettig is, omdat de personen 1) nooit zijn aangehouden of veroordeeld, en 2) niet op de hoogte zijn van het feit dat de pasfoto's van de vreemdelingenadministratie worden gebruikt voor CATCH. Zie onder andere https://www.rtlnieuws.nl/nieuws/nederland/artikel/5361083/miljoenen-pasfotos-van-onschuldige-buitenlanders-gezichtendatabase (voor het laatst geraadpleegd op 5 februari 2023).

wordt een toenemend aantal foto's verwerkt. In 2021 ging het om 1.320 aangebonden gezichtsafbeeldingen.[23] Rond de 10% hiervan leidt tot het identificeren van een verdachte. Tot hoeveel aanhoudingen of veroordelingen dit leidt, is niet bekend. Er zijn wel voorbeelden bekend waaruit blijkt dat rechters terughoudend zijn om op basis van (uitsluitend) gezichtsherkenning een uitspraak te doen.[24] Er is door de politie initiatief genomen om CATCH te vervangen door een nieuw systeem dat meer stappen geautomatiseerd uitvoert en daardoor sneller werkt.

Naast *face identification* kan gezichtsherkenning worden ingezet voor *face surveillance*: realtime gezichtsherkenning in de publieke ruimte. Dit wil zeggen dat camera's live gezichten van passerende burgers registreren en de gezichtstemplates vergelijken met de templates uit een database. In China wordt deze technologie op grote schaal in de publieke ruimte toegepast.[25] Ook in de VS grijpt deze toepassing – gedreven door technologiereuzen als Google, Microsoft, IBM, Facebook en Amazon – om zich heen, al is er ook veel kritiek op en zijn er staten die verboden hebben ingevoerd.[26] In het VK is de *Metropolitan Police* in 2021 begonnen met het gebruik van realtime gezichtsherkenning in de publieke ruimte (winkelgebieden, demonstraties).[27] Naast *face surveillance* wordt er in onder andere de VS ook gebruikgemaakt van *face tracking* om bijvoorbeeld vluchtende verdachten te volgen en te lokaliseren via videodata van verschillende camera's.[28]

De ontwikkelingen op het gebied van gezichtsherkenning gaan snel waarbij mobiele camera's de volgende stap zijn. Hierbij kan onder andere worden gedacht aan bodycams en camera's op politieauto's.[29] In China dragen (sommige) politieagenten een bril met een camera met gezichtsherkenning.[30] De agenten die deze bril op hebben, zien een klein vierkantje verschijnen rond het hoofd van degene die ze in het vizier hebben. Na een paar seconden komen de naam en het persoonlijke identificatienummer van de persoon in het scherm op de bril te staan. In die paar seconden is het opgenomen beeld door een algoritme vergeleken met de templates in een database.

De politie in Nederland mag vooralsnog geen operationeel gebruik maken van realtime gezichtsherkenning. Dit is in 2019 door de minister van Justitie & Veiligheid ge-

23 Zie de jaarcijfers 2021 die zijn gepubliceerd op www.politie.nl.
24 https://www.nu.nl/tech-achtergrond/6121506/de-impact-van-gezichtsherkenning-een-gezicht-als-bewijs-voor-criminaliteit.html (voor het laatst geraadpleegd op 2 augustus 2021).
25 https://time.com/5735411/china-surveillance-privacy-issues/ (voor het laatst geraadpleegd op 16 januari 2021). Zie ook: Gerritsen et al. 2020.
26 Zie Ferguson 2017a, 2020a.
27 https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/ (voor het laatst geraadpleegd op 16 januari 2021).
28 Zie hiervoor ook de voorbeelden in Ferguson 2020a.
29 Ferguson 2020a.
30 https://www.nytimes.com/2018/07/16/technology/china-surveillance-state.html (voor het laatst geraadpleegd op 16 januari 2021).

expliciteerd in een brief aan de Tweede Kamer.[31] De technologie voor gezichtsherkenning mag alleen worden gebruikt in de variant van CATCH. Er is in de betreffende brief door de minister een opening geboden voor breder gebruik van de technologie. Dit zou vereisen dat er degelijke waarborgen worden ingericht, inclusief juridische en ethische toetsing. Deze opening is door de politie gebruikt om de bruikbaarheid van realtime gezichtsherkenning[32] te verkennen. Ten behoeve hiervan zijn in 2020 (voorlopige) werkregels opgesteld.[33] Deze werkregels hebben onder andere betrekking op de stappen die moeten worden gezet om te kunnen experimenteren met gezichtsherkenning. Een van de voornaamste experimenteeromgevingen is het Living Lab 'Digitale Perimeter'.

Living Lab 'Digitale Perimeter'[34]
De gemeente Amsterdam, politie, Johan Cruijff ArenA en TNO werken samen aan het uitproberen van innovatieve oplossingen rondom het ArenA-terrein. Een van de projecten (van vooral de politie en TNO) heeft betrekking op gezichtsherkenning van *gezochte personen*. Het gaat dan in het bijzonder om het verkennen van de mogelijkheden om dit te doen op een manier die bijdraagt aan een optimale bescherming van de privacy.[35] Er is geëxperimenteerd met een technische oplossing die is gebaseerd op veilige verwerking van gegevens: multi-party computation (MPC).[36] Dit experiment was bedoeld om de technische haalbaarheid te valideren en de praktische bruikbaarheid te verkennen.[37] Het experiment was onderdeel van een breder onderzoek van TNO naar meer 'privacyvriendelijke' gezichtsherkenningstechnologie. Het onderzoek als geheel heeft laten zien dat nieuwe tech-

31 Zie de brief van de minister van Justitie & Veiligheid over de verwerking van persoonsgegevens in het kader van de nationale veiligheid van 20 november 2019 (32761-152).

32 Hierbij moet worden opgemerkt dat 'realtime gezichtsherkenning' nog steeds een breed begrip is, waaronder allerlei typen inzet vallen. In het vervolg zal duidelijk worden dat de inzet van de politie in Nederland vooral gericht is op opsporing van ernstige strafbare feiten.

33 Zie https://www.politie.nl/woo/korpsstaf/2022-gezichtsherkenningstechnologie.html (voor het laatst geraadpleegd op 17 juli 2023).

34 Deze inhoud is vooral gebaseerd op Van Rest et al. 2021 en Krikken 2021.

35 Dit wordt ook wel *privacy enhanced* of *privacy preserving face recognition* genoemd (zie Van Rest et al. 2021). Zie ook Borking (2010) over het gebruik van privacy enhancing technologies (PET).

36 MPC houdt in het geval van gezichtsherkenningstechnologie in dat de ene partij enkel toegang heeft tot de versleutelde gezichtstemplates die afkomstig zijn uit de livebeelden, terwijl de andere partij de sleutel voor de dataset met vooraf geregistreerde gezichtstemplates in haar bezit heeft. De vergelijking tussen de gezichtstemplates en de vooraf geregistreerde gezichten vindt plaats met de versleutelde data en enkel de uitkomst (identificatie of geen identificatie) is voor de belanghebbende partij toegankelijk. Dit maakt een minder grote inbreuk op de persoonlijke levenssfeer van mensen, omdat de partijen enkel toegang hebben tot (een deel van de) onherkenbare gezichtstemplates in plaats van daadwerkelijke gezichten. Enkel wanneer er een identificatie plaatsvindt, worden de gezichtstemplates gekoppeld aan de identiteit van een persoon. Zie verder: Van Rest et al. (2021) en ook Krikken (2021).

37 Deze fase is uitgevoerd tijdens een lockdown en had daarom het karakter van een technisch experiment op de computers van TNO (Zie Van Rest et al. 2021).

> nologie – zoals (maar niet uitsluitend) MPC – kan helpen om privacy bij gezichtsherkenning beter te beschermen.[38]

De voorlopige werkregels en uitgevoerde experimenten hebben geleid tot een landelijk kader voor de inzet van gezichtsherkenningstechnologie, dat in februari 2023 is gepubliceerd.[39] Met dit kader hoopt de politie het ministerieel 'nee' voor het gebruik van de technologie om te buigen naar een onderbouwd 'ja, mits' voor goed uitgedachte en welomlijnde gevallen, zo is in het inzetkader te lezen. Het inzetkader geeft richting aan welke wijzen van gebruik een grotere kans hebben op operationele inzet. Het gaat dan in het bijzonder om het opsporen van (ernstige) strafbare feiten die zijn gepleegd of om gevallen waarin er sprake is van een concrete dreiging van dergelijke feiten. Het inzetkader geeft tevens inzicht in de noodzakelijke randvoorwaarden waaraan moet worden voldaan om een operationele inzet van de technologie mogelijk te maken én bevat een procedure voor toetsing van de inzet van de technologie. Deze toetsing heeft betrekking op juridische regels, ethische beginselen en technische uitvoerbaarheid. Zonder een formeel instemmend besluit van de toetsingscommissie is operationele inzet van de technologie niet toegestaan. In de loop van 2023 wordt van start gegaan met een leer- en experimenteerperiode waarin wordt bekeken hoe de inhoud van het kader en de procedures werken.

Het voorgaande maakt duidelijk dat de politie in Nederland bezig is met een bredere inzet van gezichtsherkenningstechnologie in het kader van opsporing, maar mogelijk ook in het kader van de handhaving van de openbare orde of hulpverlening.[40] Duidelijk is eveneens dat de politie in Nederland goed heeft nagedacht over onder andere de proportionaliteit en subsidiariteit van deze bredere inzet.[41] Lonneke Stevens wijst erop dat dit te prijzen is, maar dat het tevens van groot belang is dat het debat niet alleen binnen de politie wordt gevoerd. Er is een breder, politiek debat nodig, zodat een geïnformeerde afweging kan worden gemaakt over alle 'kosten en baten' van de inzet van gezichtsherkenningstechnologie in de publieke ruimte.[42] Het is mijn verwachting dat dit debat in de komende jaren herhaaldelijk gevoerd zal worden, vermoedelijk vooral naar aanleiding van de operationele inzet van de technologie door de politie.

38 Zie het rapport van TNO (Van Rest et al. 2021) voor alle details. Het is in ieder geval van belang op te merken dat het bij gezichtsherkenning gaat om verschillende privacyaspecten en MPC een oplossing kan zijn voor het beter beschermen van een deel van die aspecten.

39 Politie 2023.

40 https://www.politie.nl/nieuws/2023/februari/24/00-gezichtsherkenning-mogelijk-na-voorafgaande-toets.html (voor het laatst geraadpleegd op 11 maart 2023).

41 Stevens 2023. Zie ook: https://specials.publiekdenken.nl/publiek-denken-42-2023/mark-wiebes-over-technologie-en-de-uitvoering-van-politietaken (voor het laatst geraadpleegd op 18 juli 2023).

42 Stevens 2023.

15 Drones en (andere) robots

Het waarnemen van de gang van zaken in het fysieke domein vindt tegenwoordig niet alleen plaats met slimme camera's die langs wegen hangen of mobiel zijn, maar ook vanuit de lucht met onbemande luchtvaartuigen:[1] drones. Dit hoofdstuk behandelt het gebruik van drones in het politiewerk. Het gaat daarnaast kort in op het gebruik van (andere) robots in het politiewerk.

Onbemande luchtvaartuigen

De technologie van onbemande luchtvaartuigen is oorspronkelijk ontwikkeld voor militaire doeleinden.[2] Overheden zijn drones echter ook in toenemende mate in het civiele domein gaan gebruiken, onder andere voor het politiewerk. Sinds eind 2009 zet de politie, op basis van een bijstandsaanvraag, drones van Defensie in.[3] Dit betreft in de eerste plaats de Raven: een relatief kleine drone met een warmtebeeldcamera. Deze drone werd in 2020 onder andere ingezet in experimenten in de eenheid Zeeland-West-Brabant, gericht op het toezicht vanuit de lucht op grensovergangen. Ook de grotere en meer geavanceerde ScanEagle van Defensie wordt in het kader van bijstand door de politie ingezet.[4] De ScanEagle heeft een veel langere vluchtduur dan de Raven en beschikt over een camera die geschikt is voor gezichtsherkenning.

> **Drones voor opsporing autobranden**[5]
> In juni 2019 heeft de politie in Gouda drones van Defensie ingezet ten behoeve van een opsporingsonderzoek naar autobranden. De drones vlogen gedurende een aantal weken enkele perioden over de stad en haar bewoners. De inzet van drones was één van de 'onzichtbare' maatregelen waartoe de driehoek besloot toen in Gouda auto na auto in vlammen opging. 'Je hoort ze niet en ziet ze niet, maar de drones zien wel alles. Heel scherp en tot in detail. Zelfs gezichtsherkenning is mogelijk', aldus de politiechef in

1 Eigenlijk is onbemande vliegsystemen een betere aanduiding, omdat het niet alleen gaat om het luchtvaartuig, maar ook om de bredere infrastructuur zoals het besturingssysteem en de dataverwerking.
2 Novitzky, Kokkelaar & Verbeek 2018.
3 In Amsterdam heeft men in 2006 al een drone – de AirRobot – getest voor gebruik in het politiewerk. Het betrof een test op vijf locaties. De proef heeft volgens de interne evaluatie aangetoond dat de drone 'zeer goed gebruikt kan worden bij de uitvoering van politietaken'. Het is (mij) onduidelijk of en hoe dit is verdergegaan.
4 https://www.omroepgelderland.nl/nieuws/2319066/Superdrone-Defensie-bewaakt-intocht-Nijmeegse-Vierdaagse (voor het laatst geraadpleegd op 2 augustus 2021).
5 https://www.ad.nl/gouda/defensie-drones-vlogen-boven-gouda-om-autobranden-te-stoppen-nog-nooit-eerder-vertoond (voor het laatst geraadpleegd op 3 januari 2020).

> Gouda. Om de onbemande vliegtuigen het Goudse luchtruim in te krijgen, moesten de politie en gemeente een aanvraag bij Defensie indienen. Hierbij werd – ook door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties – getoetst of aan bepaalde voorwaarden werd voldaan. Het OM beoordeelde de inbreuk op de privacy. 'Die toetsing is heel belangrijk, omdat het alle inwoners van de stad aangaat.'

De politie gebruikt niet alleen drones van Defensie, maar heeft inmiddels ook steeds meer eigen drones.[6] Het betreft inmiddels – medio 2023 – meer dan 200 drones.[7] Deze drones beschikken veelal over een camera die goed kan inzoomen en over een warmtebeeldcamera. De inzet van drones voor het politiewerk neemt bij voortduring toe. Door de inzet van drones voor het monitoren van publiek bij coronademonstraties is het gebruik meer 'op de kaart gezet', aldus een dronebestuurder van de politie.[8] Het gaat inmiddels (2022) om zo'n 2300 inzetten per jaar.[9] Iedere politie-eenheid heeft een eigen droneteam dat verantwoordelijk is voor de inzet van drones in het politiewerk. Op dit moment ligt de nadruk nog vooral op surveillance en (in mindere mate) handhavingsactiviteiten, zoals monitoren van publiek bij evenementen en demonstraties, verschaffen van overzicht van een incident, locatie of een PD[10], surveilleren van havengebieden, het op veilige afstand volgen van voer- of vaartuigen, inzet voor bewaking en beveiliging (o.a. bij het Marengo-proces) en zoeken van vermiste personen.[11] Tijdens de jaarwisseling 2022-2023 heeft de politie drones ingezet voor het surveilleren van risicogebieden. 'We kunnen daarmee heel snel zien waar iets staat te gebeuren en daarop anticiperen', zo gaf de landelijk coördinator van de politie aan.[12] Het is van belang te benadrukken dat het niet alleen om de drone zelf gaat, maar ook om de *payload*: de sensoren die onder de drone hangen. Dit betreft diverse typen camera's, maar ook andere sensoren. Sensoren worden steeds kleiner en gevoeliger waardoor ze op

6 Deze drones zijn (onder andere) van het Chinese bedrijf Da Jiang Innovations (DJI). In september 2021 publiceerde *Trouw* dat er indicaties zijn dat de data die de politie door middel van deze drones verzamelt, kunnen 'weglekken' naar de Chinese overheid. In reactie hierop stelde de politie dat zij niet kan uitsluiten dat hun data op Chinese servers terechtkomt. De drones worden daarom niet ingezet bij afgeschermde operaties, aldus de politie. Vanwege de twijfelachtige dataveiligheid maakt defensie geen gebruik van drones van DJI. Zie https://www.trouw.nl/binnenland/politie-gebruikt-chinese-drones-die-volgens-defensie-juist-onveilig-zijn-china-kan-gegevens-opvragen (voor het laatst geraadpleegd op 29 juli 2022).

7 Dit is gebaseerd op een LinkedIn-bericht van een lid van de korpsleiding met technologie, innovatie en informatie in de portefeuille.

8 https://www.at5.nl/artikelen/217676/politie-zet-steeds-vaker-drones-in-sneller-zicht-op-verdachten-en-plaats-delict (voor het laatst geraadpleegd op 3 januari 2023).

9 https://www.bndestem.nl/breda/deze-drone-geeft-de-politie-extra-ogen-met-helder-weer-kunnen-we-vanuit-breda-de-euromast-in-beeld-brengen (voor het laatst geraadpleegd op 10 juni 2023).

10 Drones worden onder andere ingezet voor 3D-opnames van een PD. Zie ook: https://www.ad.nl/gouda/moordonderzoek-in-3d-animatie-laat-rechercheurs-zien-hoe-misdaad-is-gepleegd (voor het laatst geraadpleegd op 1 augustus 2023).

11 Ik baseer me hierbij op diverse artikelen in kranten waarin de politie 'aan het woord is' over de inzet van drones.

12 https://www.nu.nl/tech/6244380/politie-zet-drones-in-voor-toezicht-tijdens-de-jaarwisseling.html (voor het laatst geraadpleegd op 3 januari 2023).

een drone kunnen worden gemonteerd en de kleinste hoeveelheden van een stof kunnen detecteren.

Snuffelen en speuren vanuit de lucht[13]

De Saxion Hogeschool en de Politieacademie hebben een gezamenlijke onderzoeksgroep *Technologies for Criminal Investigations*. Deze onderzoeksgroep werkt onder andere aan innovatieve toepassingen van onbemande luchtvaartuigen. Een van de toepassingen is een zogenaamde 'snuffeldrone' die met een combinatie van sensoren – een *e-nose* – gevaarlijke stoffen kan meten. Deze sensoren kunnen tevens meten of zich in de lucht stoffen bevinden die wijzen op de productie van (synthetische) drugs of het dumpen van drugsafval. Alle stoffen die bij de productie worden gebruikt, genereren namelijk stoffen met een uniek chemisch profiel: een *chemical fingerprint*. Door metingen te vergelijken met de (geur)profielen in een database kan, met een behoorlijke mate van waarschijnlijkheid, worden vastgesteld of er synthetische drugs worden geproduceerd.[14] Een volwaardig prototype van de snuffeldrone is op dit moment in ontwikkeling. De onderzoeksgroep heeft daarnaast, in samenwerking met het lectoraat 'Unmanned Robotic Systems' van de Saxion Hogeschool, een CSI-drone ontwikkeld die onbekende begraafplekken van vermiste personen kan zoeken c.q. detecteren.[15] De drone beschikt over een 'ground-penetrating radar' (stuurt signalen naar de grond), een hyperspectrale camera (analyseert de kleur van de vegetatie aan de oppervlakte), een thermische camera (meet afwijkingen in de bodemtemperatuur) en een gewone camera. Het is een autonome drone: door het invoeren van grenscoördinaten kan de drone systematisch over een gebied vliegen. Er is een volwaardig prototype gerealiseerd. De drone wordt doorontwikkeld met betrokkenheid van diverse partijen, waaronder de politie. Er wordt daarnaast een traject uitgevoerd gericht op protocollen, certificering en wet- en regelgeving. Gebruik van de CSI-drone is namelijk een nieuwe onderzoeksmethode.

13 https://www.exporic.nl/nl/onbemand-snuffelen-en-speuren-krijgt-nieuwe-dimensie en https://www.politieacademie.nl/Pages/Drones-als-innovatief-middel-bij-opsporing-van-drugslaboratoria-.aspx (beide voor het laatst geraadpleegd op 28 december 2021). Zie ook https://www.politieacademie.nl/lectorale-rede-jaap-knotter-techniek-voor-de-opsporingspraktijk (voor het laatst geraadpleegd op 12 oktober 2022).

14 Zie ook de video over de 'NarcoNeus' waarmee verdovende middelen kunnen worden gedetecteerd: https://www.youtube.com/watch?v=tdW6GOx8E4k (voor het laatst geraadpleegd op 18 juli 2023).

15 https://www.saxion.nl/nieuws/2023/juni/dit-is-de-toekomst-een-csi-drone-die-verborgen-graven-van-vermiste-personen-opspoort (voor het laatst geraadpleegd op 18 juli 2023).

De technologie ten behoeve van drones wordt bij voortduring doorontwikkeld.[16] Een van de ontwikkelingen is benoemd in het voorbeeld van de CSI-drone: drones worden autonomer. Dit wil zeggen dat ze automatisch vliegen en dus niet of nauwelijks hoeven te worden bestuurd. In de politie-eenheid Oost-Nederland wordt sinds 2022 in een afgeschermd gebied geëxperimenteerd met dergelijke drones.[17] Het Operationeel Centrum (OC) kan de drones activeren voor inzet bij een incident, zoals een verkeersongeval of overval. De drone vliegt dan zelf naar de betreffende locatie.[18] De videodata worden doorgestuurd naar het OC waardoor er snel een beeld kan worden gekregen van het incident. Dit beeld kan worden gebruikt voor de aansturing van de operatie door het OC.[19] Een andere ontwikkeling – die langer op zich zal laten wachten – zijn zwermdrones. Onderzoekers van de TU Delft, Radboud Universiteit Nijmegen en de Universiteit van Liverpool zijn er in geslaagd om een zwerm piepkleine drones te laten samenwerken om zelfstandig een omgeving te verkennen.[20] In de toekomst zullen zwermdrones in toenemende mate worden ingezet om rampgebieden te verkennen. Ook voor de opsporing zijn zwermdrones van meerwaarde, bijvoorbeeld als er meerdere verdachten zijn die ieder een andere kant op vluchten. Drones kunnen zich dan opsplitsen en met elkaar en het grondstation blijven communiceren.[21]

Andere robots

Drones zijn onderdeel van het wetenschappelijke vakgebied dat robotica wordt genoemd. De politie benut dit vakgebied niet alleen voor drones, maar ook voor de ontwikkeling en het gebruik van zogenaamde robothonden.[22] Een voorbeeld is de robothond Spot.

16 Zie ook https://www.trouw.nl/wetenschap/gaan-machines-zo-het-oorlogvoeren-overnemen-van-de-mens over de ontwikkeling van drones voor militaire doeleinden (voor het laatst geraadpleegd op 7 oktober 2022). Aanleiding voor het artikel zijn vier geavanceerde onbemande verkenningsvliegtuigen – MQ-9 Reaper toestellen – waarover het ministerie van Defensie in februari 2022 de beschikking kreeg. De Nederlandse Reapers zijn niet bewapend, maar de toestellen zijn er technisch gezien wel op voorbereid. Het ministerie onderzoekt de mogelijkheid van bewapening. Een Kamermeerderheid staat er in principe positief tegenover. Dit was jaren geleden ondenkbaar geweest (zie ook hoofdstuk 21), maar de oorlog in Oekraïne heeft de opvattingen van verschillende politieke partijen (vermoedelijk) beïnvloed. In mei 2023 werd naar buiten gebracht dat het ministerie van Defensie munitie heeft aangeschaft voor de MQ-9 Reaper. Zie https://www.defensie.nl/onderwerpen/materieel/nieuws/2023/05/23/defensie-schaft-munitie-voor-mq-9-reaper-aan (voor het laatst geraadpleegd op 18 juli 2023).

17 https://www.politie.nl/nieuws/2022/april/8/politie-start-met-pilot-automatische-drone.html (voor het laatst geraadpleegd op 29 juli 2022).

18 Er kijkt wel een 'vlieger' (dronebestuurder) mee vanuit een vaste werkplek. Die hoeft dus niet 'ter plaatse' te gaan, zoals op dit moment gebruikelijk is.

19 De brandweer in Twente heeft sinds medio 2023 een vergunning voor de inzet van een autonome drone. Zie https://www.tubantia.nl/enschede/landelijke-primeur-voor-brandweer-twente-automatische-drone-vliegt-voor-de-troepen-uit-naar-een-brand (voor het laatst geraadpleegd op 1 augustus 2023).

20 https://www.tudelft.nl/2019/tu-delft/zwerm-kleine-drones-verkent-onbekende-omgeving (voor het laatst geraadpleegd op 29 juli 2022).

21 Zie Custers, Oerlemans & Vergouw 2015.

22 Zie voor een internationaal perspectief: De Kool, Vermeeren & Steijn 2023.

Robothond Spot[23]

De Dienst Speciale Operaties (DSO) van de landelijke eenheid heeft in 2021 een robothond – genaamd Spot – in gebruik genomen. Deze robothond is ontwikkeld door het Amerikaanse bedrijf Boston Dynamics. Spot wordt op afstand bestuurd en kan dus niet autonoom opereren. De robothond is onder andere uitgerust met een camera en een schijnwerper en kan daarnaast worden voorzien van tal van sensoren waarmee metingen kunnen worden verricht. De robothond wordt vooralsnog vooral ingezet als middel voor verkenning, in het bijzonder om de veiligheid te beoordelen. Zo werd Spot in maart 2021 ingezet in een drugslab in Brabant – waar iemand werd aangetroffen die was overleden – om te zien of het veilig genoeg was om te betreden.[24] Er wordt dan onder andere gekeken of er druk op ketels of vaten staat, wat voor explosiegevaar zorgt. De DSO is positief over de mogelijkheden van Spot en wil er meer mee gaan experimenteren. Nederland is het enige land in Europa dat gebruikmaakt van deze robothond. In New York is de politie in 2021 juist gestopt met inzet van Spot.[25] Er was veel kritiek op de inzet. De robothond zou de verdere militarisering van de Amerikaanse politie symboliseren;[26] de vrees is dat het apparaat wordt uitgerust met wapens of explosieven.[27] Daarnaast zou de robot worden ingezet als surveillancemiddel. De politie in Nederland benadrukt dat Spot niet zal worden ingezet bij bijvoorbeeld aanhoudingen en ook geen geweld zal uitoefenen.

Kortom: de politie zet in toenemende mate robots – waaronder drones – in ten behoeve van het politiewerk.[28] Sensoren zijn hierbij cruciaal. Door middel van sensoren worden er in de fysieke wereld observaties gedaan en metingen verricht en dit leidt tot allerlei data die vervolgens verder worden verwerkt ten behoeve van het politieoptreden. De politie zet echter niet alleen technologie in om in de fysieke wereld waar te

23 Zie ook deze video: https://www.youtube.com/watch?v=IW9BjzVTUYU (voor het laatst geraadpleegd op 28 juli 2022).

24 Zie ook de video in dit bericht: https://nos.nl/artikel/2372042-dode-gevonden-bij-drugslab-in-wernhout-politie-zet-robothond-in-bij-onderzoek (voor het laatst geraadpleegd op 28 juli 2022).

25 https://www.volkskrant.nl/nieuws-achtergrond/politie-in-new-york-stopt-met-robothond-na-golf-van-kritiek-nederlandse-politie-blijft-apparaat-inzetten (voor het laatst geraadpleegd op 28 juli 2022).

26 Zie ook Balko 2013.

27 Zie ook de discussie over de inzet van robots met explosieven in San Francisco: https://www.nrc.nl/nieuws/2022/12/07/politie-in-san-francisco-mag-toch-geen-dodelijke-robots-inzetten (voor het laatst geraadpleegd op 3 januari 2023).

28 Naast hardware robots zijn er ook softwarerobots. Zo heeft men in het innovatielab in de eenheid Limburg een softwarerobot voor de afhandelingen van meldingen in het kader van Meld Misdaad Anoniem (MMA) ontwikkeld, genaamd Djack. Hierbij wordt gebruikgemaakt van Robotic Process Automation (RPA, zie ook hoofdstuk 5). De politie beschikt over een Center of Excellence op het gebied van RPA. Er zijn inmiddels zeventien robots op basis van RPA in gebruik, zo gaf een lid van de korpsleiding in juli 2023 op LinkedIn aan. En er zijn nog honderd werkprocessen in beeld waarin RPA van betekenis zou kunnen zijn. Sofwarerobots worden door de politie in Nederland ook ingezet in de vorm van chatbots, die gebruikmaken van NLP (zie hoofdstuk 5). Dit betreft in het bijzonder chatbot Wout in het kader van het afhandelen van meldingen en chatbot Job die wordt ingezet in het kader van de werving.

nemen. Er wordt ook technologie ingezet om online te monitoren en data te verzamelen. Hierover gaat het volgende hoofdstuk.

16 Online gegevensvergaring

In het eerste deel van dit boek is aan de orde gekomen dat burgers in de afgelopen twee decennia steeds meer tijd online zijn gaan doorbrengen. Het gebruik van internet in het algemeen en sociale mediaplatformen in het bijzonder is ingebed in het dagelijks leven van veel burgers. Dit impliceert dat deze platformen ook inzicht bieden in de handel en wandel van burgers.[1] De gegevens die hierover online beschikbaar zijn, kunnen voor de taakuitvoering van de politie relevant zijn.[2] De politie is in de afgelopen jaren dan ook steeds meer gaan investeren in online gegevensvergaring (OGG).[3] Dit hoofdstuk gaat in op het gebruik van technologie bij online gegevensvergaring in het kader van zowel intelligence als opsporing.

Online gegevensvergaring voor intelligence

Online vergaarde gegevens zijn in de eerste plaats een bron van intelligence. Naast allerlei menselijke bronnen van intelligence – van wijkagent tot informant – wordt door de politie gebruikgemaakt van online gegevens.[4] Internationaal staat deze praktijk ook wel bekend als OSINT: open source intelligence.[5] De rol die OSINT speelt in het opbouwen en onderhouden van intelligenceposities loopt uiteen tussen veiligheidsthema's.[6] Op het gebied van openbare orde is OSINT – zeker na project X in Haren – een belangrijke bron van intelligence, terwijl het binnen een thema als milieu een minder prominente plek inneemt. Mede als gevolg van de toenemende maatschappelijke onrust – zie hoofdstuk 8 – groeit het belang dat binnen de politie aan OSINT wordt gehecht.[7] Zo zijn sinds het uitbreken van de coronapandemie de zorgen over het anti-overheidsextremisme toegenomen.[8] Binnen het digitale ecosysteem van allerlei meer of minder extremistische groeperingen tieren allerlei complottheorieën welig en

1 Trottier & Fuchs 2015.
2 Feenstra 2018; Koops 2013; Stol & Strikwerda 2018; Trottier 2015.
3 Landman & Groothuis 2022.
4 Zie ook Miller 2018.
5 Zie Higgins 2021. Zie Block 2023 voor de historie van OSINT.
6 Zie Landman & Groothuis 2022.
7 Dit geldt niet alleen voor de politie. Uit onderzoek blijkt dat ook gemeenten op grote schaal online zijn gaan monitoren (zie Bantema et al., 2021) en in 2021 kwam in de media dat de NCTV met fake accounts burgers monitoren om zodoende de samenleving tegen dreigend onheil te beschermen. Zie voor berichtgeving over de NCTV onder andere: https://www.nrc.nl/nieuws/2021/04/09/onmin-en-uitglijders-bij-de-club-die-het-land-moet-beschermen (voor het laatst geraadpleegd op 27 juli 2022).
8 Zie Van Meeteren 2022.

worden geregeld bedreigingen tegen o.a. politici geuit en allerlei plannen besproken.[9] Het is voor de politie van belang om dit te monitoren.[10] Dit geldt in het bijzonder wanneer openbare orde-verstoringen dreigen. Door de avondklokrellen in januari 2021 werd de politie (opnieuw) met haar neus op de aanjagende rol van sociale media in openbare orde-verstoringen gedrukt.[11]

Het online vergaren van gegevens ten behoeve van intelligence vindt zowel handmatig als geautomatiseerd plaats.[12] In het kader van de geautomatiseerde vergaring maakt de politie in Nederland gebruik van diverse softwareprogramma's. Een voorbeeld is PublicSonar, dat door medewerkers van de intelligenceorganisatie en digitaal wijkagenten in de basisteams[13] wordt gebruikt.[14] PublicSonar is software die met behulp van AI fijnmazig het internet en sociale media kan scannen.[15] Dankzij algoritmen is het mogelijk om in een gigantische stroom aan data te filteren en er cruciale berichten uit te pikken.[16] Op basis hiervan kan de politie zich een beeld vormen van het sentiment rondom een bepaalde onderwerp of van een bepaalde situatie, bijvoorbeeld een demonstratie waarover op sociale media berichten verschijnen. Deze inzichten kunnen – al dan niet in combinatie met andere gegevens – worden gebruikt als basis voor het optreden van de politie in het kader van onder andere de openbare orde. Een ander voorbeeld is Maltego.[17] Maltego is een 'OSINT-tool' waarmee online gegevens kunnen worden doorzocht en kunnen worden gevisualiseerd. Zet een naam in het zoekveld en het programma zet alle gevonden data (bedrijven, locaties, e-mailadressen et cetera) die een relatie hebben met de ingevoerde naam in een diagram. Een voormalig medewerker van de politie licht de meerwaarde van deze tool toe.[18]

> *'Toen ik bij de politie werkte, op de inlichtingenafdeling bij contraterrorisme, was ik op zoek naar een terroristische cel. Het kostte me drie maanden om tot een bepaald beeld te komen. Kort daarna kreeg ik toegang tot Maltego. Toen heb ik geprobeerd hoeveel sneller ik daarmee tot hetzelfde beeld kon komen. Dat lukte binnen twee dagen.'*

9 Zie ook https://www.nctv.nl/onderwerpen/dtn/actueel-dreigingsniveau/anti-overheidsextremisme (voor het laatst geraadpleegd op 7 oktober 2022).
10 Zie ook Landman 2023.
11 Landman & Groothuis 2022.
12 Idem.
13 Zie ook Terpstra et al. 2021.
14 Landman & Groothuis 2022.
15 Zie https://publicsonar.com/nl/ (voor het laatst geraadpleegd op 5 augustus 2021).
16 Vooralsnog worden tekstberichten gescand waarbij gebruik wordt gemaakt van NLP (zie hoofdstuk 5). Het is de bedoeling dat op korte termijn ook foto's en video's kunnen worden verwerkt. Zie hiervoor: https://www.deondernemer.nl/marketing/social-media/publicsonar-social-media-data-algoritmes (voor het laatst geraadpleegd op 29 juli 2022).
17 Zie Landman & Groothuis 2022.
18 https://www.ftm.nl/artikelen/toezicht-veiligheidsdiensten-osint (voor het laatst geraadpleegd op 21 januari 2023).

Op het snijvlak van intelligence en opsporing zijn er daarnaast diverse softwareprogramma's – die veelal zijn ontwikkeld in samenwerking tussen de politie en kennisinstellingen – waarmee de politie het internet kan scannen op signalen van mogelijke criminaliteit. Ik noem drie voorbeelden:

- De webcrawler mensenhandel, die automatisch seksadvertenties kan scannen op signalen van mensenhandel. Deze webcrawler is in de afgelopen jaren voor het eerst ingezet in de voorbereiding op en uitvoering van opsporingsonderzoeken naar mensenhandel.[19]
- De Website Evaluatie Tool (WEET) die door het Landelijk Meldpunt Internetoplichting (LMIO) wordt gebruikt om webshops mee te beoordelen: is de webshop malafide of bonafide?[20] De WEET maakt gebruik van AI en geeft medewerkers suggesties voor nader onderzoek.
- De Dark Web Monitor waarmee de politie en andere opsporingsdiensten verdachte activiteiten op het darkweb kunnen detecteren.[21] Deze monitor indexeert het darkweb en maakt het mogelijk om te zoeken en geavanceerde analyses te maken.

Online gegevensvergaring ten behoeve van opsporing

Online gegevensvergaring wordt ook ingezet ten behoeve van de opsporing. In dit verband wordt er ook wel gesproken over internetrechercheren of online opsporen.[22] Internetrechercheren wordt eveneens voor de politie steeds relevanter. Dit heeft onder andere te maken met de toenemende digitale criminaliteit waarbij er niet zelden sporen online te vinden zijn.[23] Ook voor 'traditionele' criminaliteit geldt dat internetrechercheren van meerwaarde kan zijn, bijvoorbeeld voor het lokaliseren van een verdachte of het verkrijgen van een beeld van diens sociale omgeving.

Bij internetrechercheren wordt (soms) gebruikgemaakt van software voor geautomatiseerde vergaring en analyse.[24] Zo maken diverse politie-eenheden gebruik van de softwareoplossing NexusXplore,[25] die is ontwikkeld door het Australische bedrijf OSINT Combine. Met deze software kunnen op eenvoudige wijze allerlei online beschikbare gegevens – op het surface web (waaronder sociale media), deepweb en darkweb – over burgers worden vergaard en gecombineerd. Gegevens die normaal niet zichtbaar zijn, kunnen met de software zichtbaar worden gemaakt, zoals metadata. De software bevat daarnaast diverse analysemogelijkheden, waaronder sociale netwerkanalyse (zie ook hoofdstuk 18).

19 Zie bijvoorbeeld https://www.om.nl/actueel/nieuws/2022/03/22/seksuele-kinderuitbuiting-om-legt-bewijs-verzameld-door-middel-van-webcrawling-voor (voor het laatst geraadpleegd op 30 juli 2022).
20 Odekerken & Bex 2020.
21 https://www.tno.nl/nl/tno-insights/artikelen/bestrijding-cybercriminaliteit/ (voor het laatst geraadpleegd op 9 mei 2021)
22 Landman & Groothuis 2022.
23 Zie bijvoorbeeld Oerlemans 2017a.
24 Landman & Groothuis 2022.
25 Deze software kan overigens ook worden gebruikt voor intelligencevergaring.

In het kader van het gebruik van cryptovaluta voor criminele doeleinden – zie hoofdstuk 7 – is er tegenwoordig ook software beschikbaar waarmee transacties met cryptovaluta kunnen worden gemonitord, gescreend en geanalyseerd.[26] Het gaat dan in het bijzonder om bitcoin.[27] Het Amerikaanse bedrijf Chainalysis is een van de marktleiders op dit gebied en heeft diverse producten en diensten waarvan opsporingsdiensten wereldwijd gebruikmaken.[28] Met het platform en de software van Chainalysis kan de blockchain van bitcoin worden onderzocht. Een van de opgaven waarvoor de software wordt gebruikt, is het volgen van ransomware betalingen.

Opsporing van de ransomware betaling van Maastricht University[29]
In december 2019 konden de medewerkers en studenten van Maastricht University een week lang helemaal niets met de computersystemen, omdat deze waren gegijzeld. De universiteit voelde zich genoodzaakt – om tegen het advies van de politie in – het losgeld te betalen om zodoende weer beschikking te krijgen over de systemen. Het cybercrimeteam van de eenheid Limburg heeft de software van Chainalysis gebruikt om de ransomware betaling van Maastricht University op te sporen. Via het adres (de wallet) waarnaar het bedrag van 200.000 euro (30 bitcoin) is overgemaakt, verscheen in de software een netwerk van bitcoin-adressen, lijntjes en bedragen. Het bedrag is, na betaling, in drieën gesplitst en gestuurd naar nieuwe wallets. Een groot deel is vervolgens razendsnel verder gestuurd en na vele opsplitsingen nauwelijks meer te traceren. Een klein bedrag van 4,5 bitcoin kiest een andere route en gaat naar een account bij een bitcoin platform (een exchange). Dit biedt een kans. De politie vordert de gegevens van het account bij het platform. Het account blijkt van een geldezel c.q. katvanger in Oekraïne te zijn die niets van de ransomware aanval weet, maar wel onvoorzichtig is geweest door de bitcoin naar zijn eigen wallet te sturen en het vervolgens door te zetten. Deze gegevens leiden tot een nieuw spoor en dit leidt er uiteindelijk, via vele omwegen, toe dat er in april 2021 beslag kan worden gelegd op 30 bitcoin. Het losgeld is terug, maar de daders kunnen niet worden opgespoord en gepakt (zie ook hoofdstuk 6). Het vermoeden is dat de daders zich – zoals wel vaker[30] – in Rusland bevinden.

De technologie om automatisch online gegevens te vergaren, zal zich blijven ontwikkelen. Er zijn talloze bedrijven die zich bezighouden met het (door)ontwikkelen van deze technologie. Zij moeten zich van hun concurrenten onderscheiden door nog slimmere

26 Zie Schrama et al. 2022.
27 Ter herhaling: alle transacties zijn en blijven zichtbaar op de blockchain van Bitcoin; deze zijn dus openbaar. De wallets zijn veelal geanonimiseerd. Zie hoofdstuk 7.
28 Zie ook Greenberg 2022.
29 https://www.volkskrant.nl/nieuws-achtergrond/de-hackers-zijn-niet-gevangen-maar-universiteit-maastricht-heeft-wel-een-half-miljoen-aan-crypto-terug (voor het laatst geraadpleegd op 30 juli 2022).
30 Greenberg 2022.

software te ontwikkelen.[31] Het is te verwachten dat er steeds meer software zal worden ontwikkeld voor het voorspellen van gebeurtenissen.[32] Zo is er in de VS een algoritme ontwikkeld waarmee op basis van tweets geweld wordt voorspeld en zijn er politiekorpsen die realtime de samenstelling van gangs monitoren op basis van sociale media data.[33] Een tweede ontwikkeling heeft betrekking op de directe toegang dat een toenemend aantal softwareprogramma's – al dan niet via abonnementen – geeft tot datasets met persoonsgegevens die op het internet circuleren.[34] Een derde en laatste ontwikkeling zijn systemen die online vergaarde gegevens combineren met data uit onder andere sensoren en politiesystemen ten behoeve van realtime intelligence. Daarover gaat het volgende hoofdstuk.

31 Scassa 2017.

32 Zo heeft het innovatieteam (Q-LAB) van de eenheid Oost-Nederland een prototype ontwikkeld van een 'tool' voor het vroegtijdig signaleren van online opruiing.

33 Ferguson 2017a.

34 Dit is een van de grootste privacyrisico's die met online gegevensvergaring gepaard gaat. Zie onder andere het rapport van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD, 2021) over geautomatiseerde OSINT.

17 Realtime intelligence

De voorgaande hoofdstukken hebben inzicht gegeven in verschillende sensoren en (andere) toepassingen waarmee de politie zicht krijgt op de stroom van gebeurtenissen – offline en online – in de samenleving. Deze afzonderlijke datastromen worden in toenemende mate bij elkaar gebracht ten behoeve van realtime intelligence – sturingsinformatie – voor de operatie van de politie. Hierin spelen het OC en het Realtime Intelligence Center (RTIC) van de politie een belangrijke rol. In dit hoofdstuk wordt ingegaan op de ontwikkeling van deze centra in het kader van realtime intelligence.

Realtime intelligence centers in ontwikkeling

De politie heeft van oudsher een meldkamer: een plek waar centralisten werken die onder andere de spoedeisende meldingen aannemen en de noodhulpeenheden op straat aansturen.[1] Deze meldkamer heeft zich na verloop van tijd ontwikkeld tot een OC waar allerlei informatie binnenkomt en beschikbaar is – denk aan locatiegegevens van voertuigen – die wordt gebruikt om operaties van de politie aan te sturen.[2] Het gaat dan niet alleen om de noodhulp, maar bijvoorbeeld ook om evenementen en bijzondere opsporingsoperaties. Bij de vorming van de nationale politieorganisatie is er, aanvullend op het OC, een RTIC ingericht. Deze centers zijn ingericht om (meer) informatie toe te voegen aan de (spoedeisende) meldingen die binnenkomen, zodat zowel het OC als de politiemensen 'in het veld' een betere informatiepositie hebben. Medewerkers van het RTIC raadplegen hiertoe politiesystemen, systemen van partners en open bronnen.[3]

> **Het RTIC tijdens de aanslag op Peter R. de Vries**
>
> Op de bovenste verdieping van het Amsterdamse hoofdbureau zitten zo'n dertig agenten achter aaneengeschakelde computerschermen, de meesten hebben hun dienstwapen om.[4] Op de schermen: kaarten van Amsterdam, openstaande databases en een gekleurde lijst met meldingen die zojuist zijn binnengekomen via 112. Paars: moet nog behandeld worden. Groen: minder urgent. Rood: topprioriteit. Op een gigantische zwarte wand komen live

1 Zie ook Kuppens, Bervoets & Ferwerda 2010.
2 Ik beperk me hier tot de politie en haar reguliere operatie en laat de ontwikkeling van de multidisciplinaire meldkamer buiten beschouwing.
3 Scholtens, De Hengst & Waterreus 2016.
4 Deze passage is gebaseerd op https://www.nrc.nl/nieuws/2021/07/16/hoe-verdachten-aanslag-peter-r-de-vries-zo-snel-konden-worden-gearresteerd (voor het laatst geraadpleegd op 16 augustus 2021).

> camerabeelden van de hele stad voorbij. Fietsers die zoeven over een kruispunt, jongeren die hangen op de Dam, het Leidseplein. De camera's zoomen voortdurend in op personen. Dit is het RTIC van de eenheid Amsterdam. Zijn kerntaak: snel informatie verzamelen bij schietpartijen, overvallen, straatroven, huiselijk geweld en andere 112-meldingen waar iedere seconde telt. Terwijl politieagenten met loeiende sirenes op een melding afgaan, moeten de medewerkers van het RTIC binnen enkele minuten zo veel mogelijk informatie over de plek en verdachte(n) in kaart brengen. Ten behoeve hiervan raadplegen zij politiesystemen, sociale media en (andere) open bronnen. Het RTIC van Amsterdam speelde op 6 juli 2021 een cruciale rol bij de aanhouding van de verdachten van de aanslag (later moord) op Peter R. de Vries. Op camerabeelden werd de grijze Renault van de vermeende schutter gesignaleerd, maar het kenteken was niet volledig leesbaar. Door het raadplegen van systemen werd het gehele kenteken gevonden. Dit kenteken werd ingevoerd in de ANPR. Zo kon de vluchtauto worden gevolgd en op de A4 bij Leidschendam worden klemgereden.

Op dit moment wordt binnen de politie gewerkt aan het OC van de toekomst.[5] In dit centrum worden uiteenlopende databronnen – waaronder data uit sensoren, open bronnen en politiesystemen – ontsloten, gecombineerd en geanalyseerd, zodat er een doorlopend realtime intelligencepositie is waarmee de operatie kan worden aangestuurd.[6] Om dit te realiseren, vinden er verschillende ontwikkelingen plaats. Een van deze ontwikkelingen is de komst van de generieke sensingvoorziening in 2023.[7] Dit sensing platform moet de politie in staat stellen om op realtime basis datastromen te verzamelen uit verschillende soorten sensingtoepassingen (zie ook hoofdstuk 23). Hierbij worden de data op eenduidige wijze verwerkt ter ondersteuning van alle operationele politieprocessen. In 2023 komt eerst de ANPR beschikbaar (zie hoofdstuk 14). Daarna volgen steeds meer sensoren en sensortoepassingen de weg naar dit platform.

In het OC van de toekomst wordt daarnaast gebruikgemaakt van slimme software die medewerkers in hun werk ondersteunt. Deze slimme software is op dit moment in ontwikkeling. Hierbij kan worden gedacht aan een applicatie die automatisch gegevens uit open bronnen en politiesystemen verzamelt en (in samenhang) presenteert.[8] Hierdoor kunnen (veel) meer bronnen in minder tijd en met (veel) minder inspannin-

5 Voor de eenvoud van het schrijven gebruik ik hier alleen de term OC. De functionaliteit van realtime intelligence neem ik hierin mee. Ik verwacht ook dat het organisatorische onderscheid tussen het OC en het RTIC in de toekomst gaat vervagen en er meer sprake is van een frontoffice en een backoffice in het hetzelfde onderdeel. Het onderscheid tussen beide centers hangt naar mijn idee vooral samen met het gegeven dat de centra in verschillende organisatieonderdelen zijn ondergebracht: het OC bij de Dienst Operationeel Centrum (DROC) en het RTIC bij de Dienst Regionale Informatieorganisatie (DRIO).

6 Zie onder andere De Vries et al. 2018.

7 Wieland 2022.

8 Zie https://it.kombijdepolitie.nl/realtime-intelligence (voor het laatst geraadpleegd op 7 oktober 2022).

gen worden geraadpleegd. Een ander voorbeeld is een applicatie die mogelijke vluchtwegen van daders voorspelt, bijvoorbeeld bij ram- en plofkraken.

QUIN: QUestion & INvestigate[9]

QUIN is het geesteskind van Selmar Smit, een onderzoeker op het gebied van AI die werkzaam is bij TNO. De naam QUIN verwijst naar Mr. Quin uit de verhalen van Agatha Christie: een mysterieuze meneer die willekeurig opduikt om de recherchechef van aanwijzingen te voorzien ('heb je daar al aan gedacht?'). QUIN is software die kan worden gebruikt om in te schatten waar daders naartoe vluchten nadat zij een misdrijf hebben gepleegd. Het uitgangspunt hierbij is dat mensen een bepaalde voorspelbare reactie hebben als ze vluchten. De wijze waarop een delict wordt gepleegd, lijkt altijd op iets dat eerder is gebeurd. Door data uit eerdere gevallen op systematische wijze[10] op te nemen in een database en naar patronen te zoeken, kunnen regels worden bepaald waarmee de meest waarschijnlijke vluchtroutes kunnen worden berekend vanaf de locatie waar iets is gebeurd. Op basis van nieuwe gevallen kan het algoritme vervolgens worden getraind om zodoende accurater te kunnen voorspellen. Ieder incident vraagt een eigen algoritme. De QUIN-technologie is door het Nederlandse bedrijf Pandora Intelligence geïmplementeerd in de door hen ontwikkelde (voorspellende) scenario-software.[11] De (verdere) ontwikkeling vindt plaats in het zogenaamde Realtime Intelligence lab (RTI-lab) van de politie. QUIN wordt in

9 Deze beschrijving is gebaseerd op https://www.nporadio1.nl/nieuws/binnenland/tno-ontwikkelt-computermodel-om-voortvluchtige-criminelen-sneller-op-te-sporen en
https://socialmediadna.nl/quin-helpt-opsporingsteam-in-hunted en
https://beveiligingnieuws.nl/kunstmatige-intelligentie-voorspelt-vluchtroute-criminelen en
https://mtsprout.nl/management-leiderschap/scripts-als-wapen-tegen-terreur-hoe-data-science-de-wereld-veiliger-kan-maken (allemaal voor het laatst geraadpleegd op 17 oktober 2022). Luister ook naar: https://vriendvandeshow.nl/mnot/episodes/s08e03-verstoppertje-voor-volwassenen-in-hunted-en-evolutionaire-algoritmen-met-selmar-smit.

10 Hierbij wordt gebruikgemaakt van crime scripting (zie ook hoofdstuk 18): iedere zaak is opgedeeld in een aantal scenes. Binnen die scenes zijn er actoren die handelingen verrichten en hierbij gebruikmaken van bepaalde middelen. De data over de actoren en handelingen zijn geabstraheerd in de database opgeslagen en daarmee niet herleidbaar tot individuele cases. In het systeem kan een actuele zaak aan de hand van verschillende kenmerken worden ingevoerd.

11 Het scenariomodel is gebaseerd op het promotieonderzoek van de oprichter van Pandora Intelligence: Peter de Kock (2014). Dit proefschrift kan worden beschouwd als pionierswerk op het gebied van toepassing van principes van big data op scenario-ontwikkeling in de opsporing. In het onderzoek naar terroristische aanslagen is een scenariomodel ontwikkeld dat bestaat uit twaalf elementen. Door data over terroristische aanslagen uit het verleden in een database te structureren aan de hand van de twaalf elementen kunnen voor nieuwe gevallen ontbrekende elementen worden voorspeld. Bijvoorbeeld: na de aanslagen tijdens de marathon van Boston in 2013 werd al snel een foto vrijgegeven van een snelkookpan waar vermoedelijk een bom in had gezeten. Uit de analyse van de data in het systeem van De Kock kwam naar voren dat snelkookpannen een veelgebruikt wapen in Tsjetsjenië waren. Uiteindelijk bleek dat de aanslagen in Boston waren beraamd door twee Tsjetsjeense broers die in de VS studeerden. Dit voorbeeld laat zien hoe historische data met behulp van een intelligente analyse meerwaarde kunnen hebben voor de toekomst. Het scenariomodel met de twaalf elementen is inmiddels gepatenteerd en er is een scenariosoftwareplatform ontwikkeld dat gebruikmaakt van AI voor geavanceerde analyses.

> aangepaste vorm ook gebruikt in het tv-programma *Hunted* waarin deelnemers proberen om uit handen te blijven van een speciaal voor het programma opgericht opsporingsteam. Deze variant van QUIN is vooral van meerwaarde voor – en wordt gebruikt bij het opsporen van onvindbaren: personen die al zijn veroordeeld, maar zijn gevlucht en hun straf nog moeten uitzitten.[12]

Medewerkers in het OC zullen in toenemende mate worden ondersteund door slimme systemen die hen sturingsinformatie aanreiken die zij kunnen gebruiken voor aansturing van de operatie.

Verdachte situaties detecteren

Het is daarnaast waarschijnlijk dat er in toenemende mate systemen worden ontwikkeld en gebruikt die verdachte situaties in het straatbeeld detecteren. Dit wil zeggen dat algoritmen worden gebruikt om binnenkomende data te vergelijken met een profiel dat is ontwikkeld. Als de data overeenkomen met het profiel is er sprake van een 'hit': een verdachte situatie die al dan niet automatisch wordt doorgegeven aan dienstdoende politieagenten.[13] Deze manier van profilering vindt onder andere plaats met ANPR-camera's (zie hoofdstuk 14).[14] In de context van ANPR bevat een profiel vrijwel altijd meerdere plaats-/tijdgegevens of de passage van één camera op verschillende tijdstippen. Het eerste wordt een verplaatsingspatroon genoemd en het tweede een activiteitenpatroon. Aan het profiel kunnen gegevens worden toegevoegd, zoals het land waaruit een voertuig afkomstig is of persoonskenmerken van de vermoedelijke bestuurder.[15] Een ANPR-profiel wordt met crimineel gedrag geassocieerd.[16] Of er werkelijk sprake is van een (voorgenomen) strafbaar feit kan alleen met nader onderzoek worden vastgesteld. Selectie op basis van een (ANPR-)profiel verschilt dus wezenlijk van de eerder behandelde selectie op basis van een referentielijst.[17]

Het profiel wordt in de regel opgesteld op basis van expertkennis (modelgedreven in plaats van datagedreven) en gebruikt voor onder andere de aanpak van inbraak en diefstal.[18] Een voorbeeld is het initiatief *Secure Lane* waarin de politie met partners

12 Zie https://magazines.rijksoverheid.nl/jenv/jenvmagazine/2019/07 (voor het laatst geraadpleegd op 16 oktober 2022).
13 Zie ook Joh 2018b.
14 Zie Homburg et al. 2016; Niculescu-Dincă 2016.
15 Zie Niculescu-Dincă 2016 voor etnografisch onderzoek naar het gebruik van ANPR-profielen.
16 Hierbij moet worden opgemerkt dat er alleen data worden bewaard van de voertuigen die voldoen aan het profiel. Zo wordt invulling gegeven aan het principe van dataminimalisatie (zie hoofdstuk 27). De privacy-inbreuk van 'no-hit' voertuigen wordt gereduceerd – zeker ten opzichte van ongerichte 'bulkverzameling' (wat met de ANPR in Nederland verboden is) – doordat deze direct worden verwijderd. Zie verder: Niculescu-Dincă 2016.
17 Homburg et al. 2016.
18 De landelijke eenheid van de politie beschikt over een applicatie genaamde de iTrechter. In deze applicatie kunnen – nadat bepaalde procedures zijn doorlopen – profielen worden geladen waarmee analyse en alertering plaatsvinden.

samenwerkt aan de bestrijding van vrachtwagen- en ladingdiefstal. Het profiel bestaat in dit geval uit verkeersgedrag dat op ladingdiefstal kan wijzen: het binnen korte tijd bezoeken van een bepaalde parkeerplaats ('parkeerplaatshoppen').[19] Het – naar mijn idee – meest bekende voorbeeld van het detecteren van verdacht gedrag op basis van een algoritme is de proeftuin sensing voor de aanpak van mobiel banditisme in Roermond.[20]

Operationele proeftuin sensing Roermond[21]

In 2017 werd in de gemeente Roermond geconstateerd dat mobiel banditisme – internationaal rondtrekkende bendes die zich onder andere schuldig maken aan zakkenrollen – een groeiend probleem was. Om die reden is er in 2018 in Roermond een operationele proeftuin sensing ingericht waarin politie, gemeente, OM en private partners – waaronder het Designer Outlet Centre Roermond – samenwerken aan de bestrijding van mobiel banditisme. De kern van de proeftuin is vroegsignalering door middel van een sensornetwerk, zodat eerder bij een 'dreigingsontwikkeling' kan worden ingegrepen, zo valt te lezen in het plan van aanpak.[22] Anders gezegd: men wil mobiel banditisme voorkomen door potentiële daders buiten het winkelgebied van Roermond tegen te houden. Het sensornetwerk dat hiervoor wordt gebruikt, bestaat uit nieuwe en doorontwikkelde (bestaande) sensoren. In de praktijk zijn dit vooral ANPR-camera's en camera's voor merk-/model-/kleurherkenning van auto's.[23] Aan dit netwerk is intelligentie gekoppeld om het 'gedrag' van mobiel bandieten (sneller) te herkennen.[24] Dit wil zeggen dat er een algoritme is ontwikkeld dat de data analyseert en vergelijkt met een profiel. Het profiel bestaat uit een aantal kenmerken, ook wel profielregels genoemd.[25] Hoe dit profiel precies is opgebouwd, is niet bekend (zie ook hoofdstuk 29). Op basis van onderzoek van Amnesty International en de behandeling van dit onderzoek in de Tweede Kamer kan worden gesteld dat het onder andere gaat om het merk en model van het voertuig, land van herkomst van het voertuig, het aantal inzittenden en de route die het voertuig neemt.[26]

19 Zie Homburg et al. 2016.

20 De proeftuin is onder andere bekend doordat Amnesty International (2020) een kritisch rapport over de proeftuin heeft gepubliceerd.

21 Deze beschrijving is gebaseerd op verschillende bronnen waaronder het plan van aanpak van de politie van oktober 2017 (Politie 2017), het (scriptie)onderzoek van Prins (2020), het rapport van Amnesty International (2020), de behandeling van het rapport in de Tweede Kamer en de aanvullende brief van Amnesty International, een artikel in *Trouw* (https://www.trouw.nl/nieuws/met-camera-s-en-sensors-is-een-winkeldief-straks-op-grote-afstand-te-herkennen, voor het laatst geraadpleegd op 7 oktober 2022) en het artikel van Stevens et al. (2021).

22 Politie 2017: 5.

23 Prins 2020.

24 Politie 2017: 6.

25 Deze profielregels zijn gebaseerd op een literatuurstudie naar mobiel banditisme in Europa, analyse van criminaliteitsgegevens en de bevindingen van de politie op straat (zie Prins, 2020).

26 Zie ook Prins 2020.

> De analyse van de data op basis van het profiel leidt tot een risicoscore. Iedere profielregel krijgt op basis van een sensormatch een bepaalde waarde toegekend. Zo zouden mobiele bandieten vaak in een witte auto rijden van een Duits merk. Als zo'n auto richting het outletcentrum rijdt, dan levert dat punten op. Ook een Roemeens kenteken en meerdere inzittenden leveren punten op. De optelsom van de waarden die aan de verschillende profielregels zijn toegekend, bepaalt de risicoscore. Een hoge risicoscore wil zeggen dat er een aanzienlijke kans is dat de inzittenden van het betreffende voertuig bezig zijn met mobiel banditisme. Een dergelijke risicoscore leidt tot een 'hit' die wordt doorgegeven aan dienstdoende politieagenten die bepalen of zij het betreffende voertuig stilhouden en eventueel nader controleren. Wanneer zij het voertuig stilhouden, kunnen zij de resultaten hiervan vastleggen in een app op hun smartphone. Als een 'hit' na opvolging onterecht bleek (er is in de openbare documentatie niet aangegeven wanneer een hit als 'onterecht' wordt gekwalificeerd), wordt het kenteken op een whitelist geplaatst, zodat een bestuurder niet herhaaldelijk onterecht wordt stilgehouden. In 2019 bleek ongeveer 50% van de daadwerkelijke gecontroleerde voertuigen correct te zijn geselecteerd op basis van het profiel. De politie gaat ervan uit dat kwaadwillende personen na zo'n controle direct vertrekken uit Roermond. Dat is waar het om te doen is: het voorkomen van misdrijven.

De proeftuin in Roermond is inmiddels beëindigd, maar de trend is duidelijk: de politie wil steeds meer 'aan de voorkant komen' en ingrijpen voordat strafbare feiten zijn gepleegd (zie ook hoofdstuk 24). Intelligente systemen die verdachte situaties detecteren, passen in dat streven.[27] Het is daarom zeer aannemelijk dat het gebruik van intelligente systemen voor het detecteren van verdachte situaties zich verder gaat ontwikkelen.[28] Zo heeft de politie een Flexibel Reactieconcept (FRC) ontwikkeld. In dit concept heeft het vroegtijdig en geautomatiseerd detecteren van verdachte handelingen een centrale plek. Ik citeer: 'Met de inzet van meerdere sensoren (zoals slimme camera's, geluid- en gedragsherkenning) kunnen tijdig verdachte handelingen geautomatiseerd

27 Het detecteren van verdacht gedrag is in essentie een vorm van risicotaxatie. Burgers die realtime worden waargenomen, worden op basis van algoritmische analyse in een risicogroep geplaatst ten behoeve van proactief politieoptreden (zie ook Stevens et al., 2021). De proeftuin in Roermond en andere initiatieven vertonen in dat opzicht overeenkomsten met toepassingen die vallen onder de noemer van *predictive policing* (zie hoofdstuk 19). Volgens de toenmalige minister van Justitie & Veiligheid is dit overigens niet het geval. Zie hiervoor de brief van de regering in reactie op vragen n.a.v. het rapport van Amnesty International (2020) van 11 december 2020. De minister beschouwde de proeftuin in Roermond als een vorm van technologisch versterkt waarnemen. Hier slaat de minister wat mij betreft de plank mis, want het is meer dan waarnemen. Het gaat ook om betekenisgeving op basis van die waarnemingen. Een ANPR-camera op basis van een referentielijst kan nog worden beschouwd als een vorm van technologisch versterkt waarnemen, maar wanneer er een profiel wordt gebruikt dat een mogelijk verdachte situatie representeert, is er van technologisch versterkt waarnemen geen sprake meer. Het gegeven dat er ook voertuigen worden geselecteerd die uiteindelijk niet verdacht blijken te zijn, maakt het risicotaxerende karakter duidelijk. Dit komt ook naar voren in het promotieonderzoek van Niculescu-Dincă (2016).

28 Zie ook Stevens et al. 2021.

worden opgemerkt.'[29] Deze ontwikkeling is niet alleen in Nederland gaande. Het is een internationale trend. Vooral in Amerikaanse steden zijn omvangrijke sensornetwerken ontstaan, die onder andere worden gebruikt om geautomatiseerd verdachte situaties te detecteren en de politie op basis hiervan – eveneens geautomatiseerd – te activeren.[30] Ook dichter bij huis wordt geïnvesteerd in slimme systemen voor het detecteren van verdachte situaties. De Franse politie gaat vanaf eind juni 2023 twee jaar experimenteren met het gebruik van AI voor het analyseren van videobeelden teneinde 'verdachte bewegingen in mensenmassa's te identificeren'.[31] Begin 2023 is er wetgeving aangenomen voor het experimenteel gebruik van AI voor het detecteren van verdachte situaties bij grootschalige evenementen waarbij het gebruik van gezichtsherkenning expliciet wordt uitgesloten.[32] Deze stap is gezet met het oog op de Olympische Spelen, die in de zomer van 2024 in Parijs plaatsvinden. Frankrijk is het eerste land dat AI met dit doeleinde op grote schaal inzet. Er is – gezien de eerder beschreven trend – reden om aan te nemen dat het niet het laatste land zal zijn.[33]

29 Zie de brief van de minister van Justitie & Veiligheid over de voortgang van de versterking van het stelsel van bewaken & beveiligen van 14 april 2022.

30 Zie Burrington 2016; Ferguson 2017a; Ferguson 2020b; Levine et al. 2017.

31 https://www.ad.nl/tech/na-chaos-cl-finale-hoopt-franse-regering-bij-spelen-in-parijs-op-videobewaking-met-kunstmatige-intelligentie (voor het laatst geraadpleegd op 22 februari 2023).

32 Zie https://www.theguardian.com/world/2023/may/18/french-courts-approval-of-olympics-ai-surveillance-plan-fuels-privacy-concerns (voor het laatst geraadpleegd op 22 juli 2023).

33 Dit is een van de redenen dat de ontwikkeling in Franrijk op veel weerstand stuit van groepen en organisaties die opkomen voor mensenrechten: de ervaring leert dat maatregelen die als uitzondering worden ingezet op termijn worden genormaliseerd. Zie: https://www.bbc.com/news/world-europe-66122743 (voor het laatst geraadpleegd op 22 juli 2023).

18 Veiligheidsanalyse

De exponentiële toename van beschikbare data en opkomende technologieën waarmee deze data kunnen worden verwerkt, zijn van grote waarde voor analyse het kader van intelligence.[1] Analyse ten behoeve van intelligence heeft verschillende verschijningsvormen. Een van de verschijningsvormen is veiligheidsanalyse.[2] Dit betreft het analyseren van veiligheidsvraagstukken ten behoeve van de sturing op strategisch, tactisch en operationeel niveau. Dergelijke veiligheidsanalyses spelen een belangrijke rol in de aanpak van (onder andere) georganiseerde criminaliteit. Door middel van veiligheidsanalyse wordt beoogd om meer inzicht te krijgen in de criminele wereld. Dit inzicht kan vervolgens worden gebruikt om criminele netwerken en processen te verstoren.[3] Het tegenhouden van criminaliteit is hierbij het streven (zie ook hoofdstuk 24 en 26). Dit hoofdstuk gaat in op de rol van technologie bij veiligheidsanalyse.

Methoden voor veiligheidsanalyse

In de wetenschap zijn diverse methoden ontwikkeld waarmee de criminele wereld in kaart kan worden gebracht. Dit is in de eerste plaats *crime scripting*.[4] Een crime script beschrijft het criminele proces om een delict te plegen.[5] Het perspectief is dat van de (aspirerend) crimineel. Met een crime script worden kennis en informatie over de 'procedurele aspecten' van specifieke vormen van criminaliteit systematisch gebundeld, georganiseerd en inzichtelijk gemaakt.[6] Hierbij wordt het criminele proces opgedeeld in stappen en rollen die binnen iedere stap van belang zijn. Bijvoorbeeld: de cocaïnehandel bestaat uit verschillende scripts, waaronder de invoer via zeecontainers.[7] De invoer is vervolgens weer onder te verdelen in allerlei activiteiten en rollen, bijvoorbeeld personen die ervoor zorgen dat de cocaïne onopgemerkt langs controlepunten komt. Een rol kan vervolgens worden ingevuld met specifieke personen – in politietaal 'subjecten' – die deze rol vervullen. Op basis van een crime script kan worden gekeken naar aangrijpingspunten om het criminele proces te verstoren via barrières of via het aanpakken van subjecten die veel waarde toevoegen in het criminele

1 Bland 2022; Kirby & Keay 2021.
2 Reijneveld 2017.
3 Kop 2012.
4 Zie Snaphaan 2021 voor (onder andere) een historisch perspectief op crime scripting.
5 Lavorgna 2019.
6 Cornish 1994.
7 Zie bijvoorbeeld Staring et al. 2019.

proces en moeilijk vervangbaar zijn.[8] Er wordt onder andere door Europol vanuit gegaan dat het aanpakken van deze *high value targets* zorgt voor '… a stronger and more disruptive law enforcement response'.[9]

Naast crime scripting is sociale netwerkanalyse (SNA) een methode in opkomst. Door middel van SNA kunnen verschillende elementen van een crimineel netwerk worden geïdentificeerd en relaties tussen netwerken worden blootgelegd.[10] Het in kaart brengen van criminele netwerken is van alle tijden: wie maffiafilms uit de jaren zeventig en tachtig van de vorige eeuw kijkt, ziet in een politiebureau altijd wel ergens een overzicht van de (bekende) leden van de criminele organisatie hangen, bestaande uit verschillende lagen, met getekende pijlen tussen personen. SNA is hier een geavanceerde versie van waarbij wiskundige formules worden gebruikt om allerlei netwerkwaarden te berekenen, *onder andere* gericht op het identificeren van sleutelpersonen in het criminele netwerk.[11] In de afgelopen jaren zijn steeds meer toepassingen of tools beschikbaar gekomen voor het uitvoeren van geavanceerde sociale netwerkanalyses, waaronder graph modelling waarmee relaties tussen entiteiten (personen, bedrijven, plaatsen et cetera) kunnen worden gevisualiseerd.[12]

Classificeren van data

Data over de criminele wereld heeft in de regel het karakter van ongestructureerde data. Het gaat dan veelal om gegevens in criminele informatierapporten, mutaties, allerlei gegevensdragers, cryptocommunicatiedata (chats) en dergelijke. Om deze data te kunnen gebruiken voor het opbouwen en onderhouden van een intelligencepositie is het nodig om deze te classificeren of labelen, zodat een gestructureerde en op grotere schaal analyseerbare dataset ontstaat. In dit kader is er door de politie in Nederland een classificatiemethode ontwikkeld, genaamd Hyperion.

Hyperion[13]

Hyperion is ontwikkeld door de Teams Criminele Inlichtingen (TCI).[14] Hyperion is gebaseerd op crime scripting en SNA. De methode bestaat uit een gestandaardiseerd classificatiemodel met hoofdclassificaties – waaronder markten, rollen, fasen criminele proces, locaties, landen – die zijn onderverdeeld in subclassificaties. Zo zijn er per markt en per fase diverse rollen gedefinieerd, bijvoorbeeld financiers en specifieke facilitators. Het is een dynamisch model, wat wil zeggen dat het met enige regelmaat wordt aangepast

8 In het kader van 'follow the money' is 'financial crime scripting' in opkomst. Met deze variant van crime scripting kunnen geldstromen worden onderzocht en financiële structuren worden blootgelegd. Zie bijvoorbeeld Van Santvoord & Van Ruitenburg 2022.
9 Europol 2021a: 22.
10 Bichler & Malm 2019; Van der Hulst 2008.
11 Zie bijvoorbeeld Ariel 2019; Bichler 2019; Knoke 2015; Vermeulen, Sodijn & Van der Leest 2021.
12 Bichler 2019.
13 Van der Plas & Brown 2017.
14 Zie Den Hengst et al. 2015 voor (enkele) achtergronden bij de ontwikkeling van Hyperion.

op basis van ervaringen in de praktijk. Hyperion wordt gebruikt om ongestructureerde data – opgenomen in criminele informatierapporten – te classificeren, zodat gestructureerde data ontstaan.[15] Door de data op gestandaardiseerde wijze te classificeren en in een relationele database op te nemen, wordt er een analytische dataset gecreëerd die kan worden benut om de criminele wereld inzichtelijk te maken. De kernvragen hierbij zijn: wie doet wat en waar? Deze dataset wordt onder andere gebruikt om het Nationaal Inlichtingenbeeld Ondermijning (NIBO) op te stellen. In het NIBO wordt een samenhangend beeld van de criminele wereld gepresenteerd (strategische analyse).[16] De dataset van het NIBO kan ook worden gebruikt voor het maken van tactische en operationele analyses, bijvoorbeeld het identificeren van sleutelpersonen in een bepaalde markt.

Het gebruik van Hyperion heeft zich in de afgelopen jaren uitgebreid van de TCI naar het bredere intelligencedomein binnen de politie. Dit heeft als gevolg dat niet alleen data uit de criminele informatierapporten worden gebruikt, maar ook data die worden gegenereerd in de basispolitiezorg en binnen de rechercheonderdelen.[17] Dit worden ook wel artikel 8 (dagelijkse politietaak), artikel 9 (uitgebreidere opsporingsonderzoeken) en artikel 10 (opbouwen informatiepositie door inlichtingen) gegevens genoemd. Hiermee wordt verwezen naar de artikelen uit de Wet politiegegevens (Wpg) waarin de verwerking van deze gegevens is gereguleerd (zie ook hoofdstuk 27).

De hiervoor genoemde data zijn opgeslagen in databases van de registratiesystemen. De data uit de verschillende bronnen worden in toenemende mate[18] geëxtraheerd, geclassificeerd en gecombineerd in (relationele) databases of datawarehouses. Zo ontstaat een gestructureerde intelligencepositie[19] op basis waarvan analyses kunnen plaatsvinden. Hierbij is het streven om data voortdurend te extraheren, classificeren en combineren, zodat de intelligencepositie zo actueel mogelijk is.[20] De intelligencepositie wordt gebruikt om – door middel van analyse – veiligheidsbeelden te maken waarin criminele netwerken en criminele processen inzichtelijk worden gemaakt. Een dergelijk beeld kan voor verschillende doeleinden worden gemaakt: prioriteren van veiligheidsproblemen (strategisch), ontwikkelen van een probleemgerichte aanpak voor een specifiek veiligheidsprobleem (tactisch) en starten van interventies, waaron-

15 Het is, naast een analysemethode, dus ook een datamodel.
16 Klerks & Vink-Teeven 2020.
17 Idem.
18 Er doen zich verschillen voor tussen veiligheidsthema's en eenheden.
19 Dit is een van de langetermijnontwikkelopgaven van de politie in het intelligencedomein. Zie bijvoorbeeld de jaarverantwoording 2020.
20 Continue classificering is niet altijd en overal vanzelfsprekend, mede omdat het arbeidsintensief is. Daarnaast: een actueel veiligheidsbeeld wil zeggen dat alle relevante data erin zijn opgenomen. Dit wil niet zeggen dat de data betrekking hebben op wat er nu plaatsvindt, want in bijvoorbeeld een opsporingsonderzoek wordt in de regel het verleden gereconstrueerd.

der opsporingsonderzoek (operationeel).[21] Een veiligheidsbeeld kan tevens worden gebruikt om incidenten die plaatsvinden te duiden.[22] Bijvoorbeeld: er wordt een dode man op straat aangetroffen die snel wordt geïdentificeerd. Het raadplegen van het veiligheidsbeeld maakt duidelijk dat de man een sleutelspeler is in een crimineel netwerk en gebrouilleerd is geraakt met een andere sleutelspeler. Dit inzicht draagt bij aan het ontwikkelen van scenario's en hypothesen over wat er mogelijk is gebeurd.

Veiligheidsanalyse en probleemgerichte aanpak

Een gestructureerde intelligencepositie kan – zoals hiervoor is aangegeven – worden gebruikt om te komen tot een probleemgerichte aanpak van (georganiseerde) criminaliteit. In de afgelopen jaren zijn dergelijke probleemgerichte, integrale aanpakken van georganiseerde criminaliteit in toenemende mate tot stand gekomen.[23] Het gaat hierbij om de aanpak van zowel de traditionele, georganiseerde criminaliteit als de georganiseerde cybercriminaliteit.

Integraal bestrijdingsmodel cybercriminaliteit[24]

Het THTC van de politie is jaren geleden gestart met een project genaamd The Incredible Machine (TIM). Dit project heeft geleid tot een 'datagedreven' aanpak van cybercriminaliteit waarin onderscheid wordt gemaakt tussen vier fasen: collect, store, analyse en engage (CSAE, uitspraak: seesay). Dit werkproces is ontstaan vanuit de behoefte om een betere informatiepositie op te bouwen door data te structureren en bij elkaar te brengen in een datawarehouse. Dit betreft data uit opsporingsonderzoeken en andere bronnen, waaronder online gegevens. Deze data worden onder andere geordend in crime scripts, ook wel 'book of crime' genoemd.[25] De opgebouwde informatie- of intelligencepositie wordt onder andere gebruikt om zicht te krijgen op cybercriminele fenomenen en (nieuwe) interventies te ontwikkelen voor de bestrijding. Het belang van andere (dan strafrechtelijke) interventies is bij de aanpak van cybercriminaliteit groot, omdat opsporing en vervolging van (veelal) internationaal opererende cybercriminelen uitdagend is en succes zeker niet is gegarandeerd (zie ook hoofdstuk 6). In de interventiefase van de aanpak – engagement – wordt gebruikgemaakt van een 'integraal bestrijdingsmodel'. Dit model bestaat uit verschillende elementen: a) attributie (opsporing & vervolging), b) verstoring van het criminele proces, c) slachtofferhulp en d) mitigatie of schadebeperking. De verschillende

21 De cryptocommunicatiedata zijn hiervoor van belang, omdat deze data hebben gezorgd voor veel informatie over de subjecten die bepaalde rollen vervullen (zie ook hoofdstuk 12). Deze data kunnen – onder voorwaarden – worden gebruikt om opsporingsonderzoek te starten en als bewijs dienen.

22 Zie bijvoorbeeld dit interview met de portefeuillehouder opsporing: https://www.regioburgemeesters.nl/actueel/?id=752 (voor het laatst geraadpleegd op 8 oktober 2022).

23 Zie bijvoorbeeld Nelen et al. 2023 die opmerken dat Nederland – in vergelijking tot buurlanden – vooroploopt in de probleemgerichte aanpak van (georganiseerde) criminaliteit.

24 Deze uitwerking is vooral gebaseerd op Van den Eeden et al. 2021 en Van de Sandt et al. 2022.

25 Swinkels & van Zwieten 2022.

typen interventies gaan vaak hand in hand, bijvoorbeeld door opsporingsonderzoek te combineren met verstoring.[26]

In de afgelopen jaren zijn diverse (internationale) operaties uitgevoerd waarin verstoring een belangrijk element was. Operatie 'Bayonet' – waarbij het THTC de controle over de toonaangevende Hansa Market had overgenomen en gedurende een maand als beheerder heeft gefunctioneerd – was in 2017 baandoorbrekend.[27] Meer recent kan worden gedacht aan de operatie Power OFF waarbij ongeveer vijftig van 's werelds grootste DDoS-for-hire websites offline zijn gehaald,[28] het neerhalen van de HIVE-infrastructuur voor ransomware[29] en het uit de lucht halen van de spoofingdienst iSpoof (in het kader van bankhelpdeskfraude).[30] Bij dergelijke operaties vinden er ook vaak 'knock and talk'-acties plaats waarbij de gebruikers van illegale diensten (onder wie jongeren) een waarschuwingsgesprek krijgen om hen af te schrikken en te laten zien dat de politie toezicht houdt.[31] De politie in Nederland loopt voorop met (de bijdrage aan) dit soort operaties.[32] In de wetenschappelijke literatuur wordt ervan uitgegaan dat dergelijke operaties – mede vanwege de belemmeringen bij (uitsluitend) opsporing en vervolging – relatief effectief zijn.[33] Er is echter ook discussie over.[34] Er wordt gewerkt in 'grijs gebied', omdat (bijzondere) opsporingsbevoegdheden worden ingezet om te verstoren. De inzet van dergelijke bevoegdheden drijft zo af van het oorspronkelijke doel: materiële waarheidsvinding.[35] De strafvorderlijke normering is op dit oorspronkelijke doel afgestemd. Voor de inzet van bijzondere opsporingsbevoegdheden ten behoeve van verstoring bestaat dan ook geen wettelijke grondslag.[36] Het ontbreekt daarnaast aan ex-post toetsing – door een rechter – wanneer de zaak niet ter

26 Hirsch Ballin & Oerlemans 2023.

27 Operatie Bayonet was breder dan de overname van de Hansa Market. De operatie betrof een samenwerking tussen de FBI en het THTC gericht op AlphaBay en Hansa Market. De Hansa Market is na de betreffende maand ook offline gehaald (AlphaBay was al eerder offline gehaald, zodat de gebruikers deels overgingen naar Hansa Market die onder controle was van het THTC). Zie verder: Oerlemans & Van Wegberg (2019).

28 https://www.politie.nl/nieuws/2022/december/15/03-politieorganisaties-wereldwijd-zetten-strijd-tegen-ddos-for-hire-websites-voort.html (voor het laatst geraadpleegd op 17 januari 2023).

29 https://www.europol.europa.eu/media-press/newsroom/news/cybercriminals-stung-hive-infrastructure-shut-down (voor het laatst geraadpleegd op 29 januari 2023).

30 https://www.politie.nl/nieuws/2022/november/23/03-grote-spoofingdienst-uit-de-lucht-gehaald-door-internationale-samenwerking.html (voor het laatst geraadpleegd op 21 januari 2023).

31 Zie ook Hirsch Ballin & Oerlemans 2023.

32 https://www.ftm.nl/artikelen/ransomware-bende-deadbolt-politie (voor het laatst geraadpleegd op 17 januari 2023); zie ook Oerlemans & Van Wegberg 2019.

33 Collier et al. 2022.

34 Zie onder andere Schermer 2022.

35 Hirsch Ballin & Oerlemans 2023.

36 De Commissie-Koops (2018) heeft in dit kader geadviseerd om de eventuele inzet van bijzondere opsporingsbevoegdheden voor intelligence- en verstoringsdoeleinden (in bepaalde omstandigheden) wettelijk te regelen. Een dergelijke regeling moet dan ook voorzien in de wijze waarop toetsing – bij het ontbreken van vervolging en een terechtzitting – invulling moet krijgen (zie ook Schermer, 2022).

zitting wordt gebracht.[37] Kortom: het Wetboek van Strafvordering sluit – ook in de gemoderniseerde variant – niet aan bij het bredere opsporingsbegrip dat zich in de praktijk heeft ontwikkeld (zie ook hoofdstuk 27).

Toekomstige ontwikkelingen

Het extraheren en classificeren van data is op dit moment een (zeer) arbeidsintensief proces.[38] De geclassificeerde data uit diverse systemen komen daarnaast terecht in afzonderlijke databases of warehouses op eenheids-, thema- of afdelingsniveau. Onder de noemer van Helios werkt de politie in Nederland op dit moment aan het aanpakken van deze kwesties.[39] Helios staat voor de ambitie om te komen tot één werkproces voor de intelligencecyclus en één intelligencedatabase waarmee alle politiemedewerkers gaan werken. Het is in dat opzicht een big data-ontwikkeling.[40] Er is een applicatie ontwikkeld die kan worden gebruikt voor het classificeren van data op basis van (onder andere) het datamodel van Hyperion. Helios zoekt iedere nacht automatisch in de registratiesystemen – op dit moment nog vooral artikel 8-registraties – naar registraties die relevant zijn voor een bepaald veiligheidsthema.[41] Hierbij wordt gebruikgemaakt van een woordenlijst. Een intelligencemedewerker leest de gevonden teksten en labelt deze handmatig via de keuzemenu's van de applicatie (bijvoorbeeld de keuze van een rol). Helios wordt stapsgewijs verder ontwikkeld waarbij het steeds verder automatiseren van het structureren van de data het streven is. Hierbij moet onder andere worden gedacht aan het prioriteren van de geëxtraheerde data en het eventuele gebruik van machine learning algoritmen voor classificatie.[42] Parallel aan de (door)ontwikkeling van Helios wordt binnen de politie gewerkt aan de verdere ontwikkeling en verspreiding van het CSAE-werkproces en het datawarehouse in het kader van de aanpak van (onder andere) cybercriminaliteit.[43]

In de toekomst is een aantal (verdere) ontwikkelingen waarschijnlijk. Het gaat allereerst om het gebruiken en combineren van data uit steeds meer bronnen. Hoewel op dit moment de data uit verschillende basis- of bedrijfsprocessensystemen met elkaar worden gecombineerd, moet worden beseft dat er nog veel meer gegevens zijn die voor veiligheidsanalyse relevant kunnen zijn. Dit betreft in de eerste plaats de data die digitaal forensisch zijn veilig gesteld, maar niet in processen-verbaal en het bedrijfsproces-

37 Dit speelt vooral bij bijzondere opsporingsbevoegdheden die op bevel van uitsluitend de officier van justitie kunnen worden ingezet en (dus) geen bevel van de rechter-commissaris vereisen (zie Schermer, 2022).

38 Klerks & Vink-Teeven 2020.

39 Zie de eerste editie van het magazine *Scherp over intelligencegestuurd politiewerk*: https://www.regioburgemeesters.nl/actueel/?id=799 (voor het laatst geraadpleegd op 7 oktober 2022).

40 Zie hiervoor ook het verslag van de bijeenkomst van de vaste Kamercommissie Digitale Zaken die heeft plaatsgevonden op 14 november 2022: https://www.tweedekamer.nl/kamerstukken/commissieverslagen/detail?id=2022Z21400&did=2022D50031 (voor het laatst geraadpleegd op 3 januari 2023).

41 Zie de derde editie van het magazine *Scherp over intelligencegestuurd politiewerk* (juli 2023).

42 Classificatie van teksten uit registraties is overigens een voorbeeld van een taak waar veel contextuele kennis voor nodig is. Dit impliceert dat automatische classificatie vooralsnog grenzen heeft.

43 Zie Kroes et al. 2023.

systeem van de opsporing (Summ-IT) terecht zijn gekomen (artikel 9-gegevens).[44] Het gaat dan om data uit onder andere uitgelezen telefoons, laptops en andere apparaten. Deze data staan in een aparte omgeving. Het is op dit moment technisch niet mogelijk om deze gegevens te benutten voor veiligheidsanalyse, al is het THTC hierop een uitzondering. Een vergelijkbare situatie doet zich voor bij data uit fysiek forensisch onderzoek. Ook deze data zijn opgeslagen in een aparte omgeving en kunnen niet (op grote schaal) als *forensic intelligence* worden gecombineerd met andere intelligencebronnen.[45] Een derde bron waaraan kan worden gedacht betreft online vergaarde gegevens. Ook deze worden op dit moment nog niet meegenomen in intelligencedatabases. In alle gevallen geldt dat rekening moet worden gehouden met wat (vooralsnog) juridisch mogelijk is en de eventuele onduidelijkheden die op dit gebied bestaan (zie ook hoofdstuk 27). Een tweede ontwikkeling is het toenemend gebruik van AI voor veiligheidsanalyse.[46] Dit gebruik staat nu nog in de kinderschoenen.[47] De potentie van AI heeft betrekking op het extraheren, classificeren, analyseren en visualiseren[48] in het kader van veiligheidsanalyse. De toekomst moet uitwijzen in welke mate en op welke wijze (machine learning) algoritmen hier een (verdere) rol in kunnen spelen, al dan niet met een *human-in-the-loop* voor controle. Een derde en laatste ontwikkeling is *anticipatory intelligence*.[49] Dit betreft vooruitkijken naar opkomende trends en ontwikkelingen én het inschatten van effecten van interventies op de korte en lange termijn, bijvoorbeeld: wat gaat er waarschijnlijk gebeuren als je de rol van facilitator X in het criminele netwerk beëindigt? Het maken van zulke inschattingen is van belang om georganiseerde criminaliteit duurzaam tegen te houden.

Met het benoemen van voorspellende mogelijkheden zijn we aanbeland bij het laatste hoofdstuk van dit deel van het boek.

44 Zie ook Roest 2023.
45 Hierbij kan onder andere worden gedacht aan het gebruik van forensische sporen die op productielocaties van synthetische drugs worden aangetroffen ten behoeve van het kaart brengen van criminele samenwerkingsverbanden. Zie bijvoorbeeld: Rossy & Morselli (2018).
46 Ariel 2019.
47 Zie hiervoor het verslag van de bijeenkomst van de vaste Kamercommissie Digitale Zaken die heeft plaatsgevonden op 14 november 2022: https://www.tweedekamer.nl/kamerstukken/commissieverslagen/detail?id=-2022Z21400&did=2022D50031 (voor het laatst geraadpleegd op 3 januari 2023).
48 Zie bijvoorbeeld Dreżewskia, Sepielaka & Filipkowskib 2015; Robison & Scogings 2018.
49 Barros 2022; Barros et al. 2022.

19 Predictive policing

Een van de meest meeslepende ideeën die voortvloeit uit het gebruik van AI in het politiewerk is de mogelijkheid om criminaliteit te voorspellen en deze voorspellingen te gebruiken om te anticiperen op criminaliteit die gaat plaatsvinden.[1] Dit idee is in het afgelopen decennium in een groot aantal landen tot ontwikkeling gekomen onder de noemer van *predictive policing*.[2] Politieorganisaties wereldwijd hebben hoge verwachtingen van dit concept.[3] Dit hoofdstuk behandelt dit concept door achtereenvolgens in te gaan op de definitie, twee verschijningsvormen en de doorontwikkeling.

Predictive policing op hoofdlijnen

Er is geen eenduidige definitie van predictive policing voorhanden, maar er is in de literatuur wel een behoorlijke mate van overeenstemming over de kernelementen van dit concept. Deze kunnen worden teruggebracht tot twee hoofdkenmerken.[4] Het eerste kenmerk is het gebruik van algoritmen om op basis van veel en gevarieerde data criminaliteit in de nabije toekomst te voorspellen. Het tweede kenmerk is het ondersteunen van de besluitvorming met betrekking tot inzet en acties van politiemensen op basis van de voorspelde criminaliteit. De volgende definitie geeft de essentie van predictive policing naar mijn idee goed weer:

> *'… I understand predictive policing as a policing strategy that uses algorithmic surveillance to predict future crimes, criminals, and victims to intervene before crimes occur.'*[5]

De definitie laat zien dat het voorspellen van criminaliteit breed moet worden opgevat. Het gaat niet alleen om delicten, maar ook om potentiële daders en slachtoffers. Het onderscheid tussen delicten en individuen – of het nu daders of slachtoffers zijn – is de basis voor de twee verschijningsvormen van predictive policing: *predictive mapping* en *predictive identification*.[6] Beide vormen worden in dit hoofdstuk nader toegelicht. De definitie laat tevens zien dat het een strategie is. Predictive policing is dus meer dan de

1 Ferguson 2017b.
2 Meijer & Wessels 2019
3 Ferguson 2017b; Meijer & Wessels 2019.
4 Meijer & Wessels 2019.
5 Van Brakel 2021.
6 Zie van Brakel 2016; Rienks & Schuilenburg 2020.

technologie en de voorspellingen zelf; het is een operationele strategie.[7] De strategie is gericht op het voorkomen van criminaliteit. In het Nederlandse taalgebruik is hiervoor de term 'preventie' gangbaar. Toch kan deze term misleidend zijn, omdat dit kan worden begrepen als het beïnvloeden van de oorzaken van criminaliteit. In het kader van predictive policing heeft preventie een specifiekere betekenis. In het Engels wordt hier de term *pre-emptive* voor gebruikt: inzicht verkrijgen in wat er gaat gebeuren en ingrijpen voordat het gebeurt (zie ook hoofdstuk 24).[8] Het is tot slot van belang op te merken dat het basisidee van predictive policing niet nieuw is. De introductie van predictive policing past in een ontwikkeling om politieprestaties te verbeteren via het gebruik van data en doen van voorspellingen.[9] Nieuw is het gebruik van AI (zie ook hoofdstuk 22).

Predictive mapping

Predictive mapping is de meest gebruikte vorm van predictive policing.[10] In 2011 is het politiekorps in Los Angeles begonnen met predictive mapping. Hierbij werd gebruikgemaakt van het programma *PredPol,* dat in handen is van het gelijknamige bedrijf.[11] Na een ogenschijnlijk succesvol experiment heeft het gebruik van PredPol zich snel verspreid onder politiekorpsen in zowel de VS als in andere (vaak Angelsaksische) landen, waaronder het VK. In continentaal Europa zijn in het afgelopen decennium allerlei eigen systemen, al dan niet gebaseerd op software van bedrijven, ontwikkeld. Dit betreft onder andere Denemarken, Duitsland, Zwitserland, Italië en Spanje.[12]

De systemen die in het binnen- en buitenland worden gebruikt om (plaatsgebonden) delicten te voorspellen, werken allemaal op een *enigszins* vergelijkbare manier.[13] Het hart van het systeem wordt gevormd door algoritmen die op basis van verschillende variabelen berekenen welke kans er is dat er in een bepaalde periode op een bepaalde plaats bepaalde delicten worden gepleegd. De gedachte hierachter is dat criminaliteit bepaalde patronen volgt en een zekere mate van voorspelbaarheid heeft. Deze patronen worden in de regel door het systeem geïdentificeerd door middel van datamining: aan de hand van een of meer methoden wordt in een berg data naar correlaties gezocht om zodoende variabelen te identificeren die significant samenhangen met delicten die hebben plaatsgevonden (*predictoren).*[14] De patronen die in de data worden gevonden, worden vervolgens gebruikt om de kans te berekenen dat bepaalde criminaliteit zich

7 Ratcliffe 2019.
8 Van Brakel 2021; zie ook Meijer & Wessels 2019.
9 Van Brakel 2021; Brayne 2021; Egbert & Leese 2021; Rienks & Schuilenburg 2020; Waardenburg, Sergeeva & Huysman 2020.
10 Van Brakel 2021.
11 Het korps in Los Angeles is inmiddels gestopt met PredPol. In de publieke berichtgeving werden bezuinigingen als belangrijkste reden hiervoor gegeven. Wie dieper graaft, moet concluderen dat men ook heeft geconstateerd dat er geen overtuigende aanwijzingen zijn dat PredPol en de daarop gebaseerde (preventieve) manier van werken hebben bijgedragen aan het reduceren van criminaliteit (zie Terpstra & Salet 2023).
12 Van Brakel 2021; Egbert & Leese 2021; De Kool, Vermeeren & Steijn 2023.
13 Zie ook Snaphaan, Hardyns & Ponnet 2021.
14 Mali, Bronkhorst-Giesen & Den Hengst 2017.

op bepaalde plaatsen voordoet.[15] Bijvoorbeeld: als blijkt dat er bij regen stelselmatig minder wordt ingebroken, dan wordt deze factor meegenomen in de berekening. Uit verschillende onderzoeken komt naar voren dat de algoritmen die op basis van datamining ontstaan om plaatsgebonden delicten te voorspellen in de regel worden ondersteund door criminologische theorieën waarvoor ook (enig) empirisch bewijs aanwezig is.[16] Een voorbeeld van zo'n theorie is het *near repeat effect*: als er in een wijk wordt ingebroken in een huis, dan is er in die wijk in de dagen daarna een verhoogde kans op woninginbraken.[17]

Op hoofdlijnen zijn er twee hoofdgroepen variabelen te onderscheiden die (veelal) door het systeem worden gebruikt om patronen te zoeken en voorspellingen te genereren. De eerste hoofdgroep betreft variabelen over de criminaliteit die heeft plaatsgevonden. Het gaat hierbij onder andere over de dagen en tijden waarop bepaalde delicten op bepaalde locaties hebben plaatsgevonden. De tweede hoofdgroep heeft betrekking op variabelen over het gebied waarop een voorspelling van criminaliteit betrekking heeft. Het betreft een groot aantal (mogelijke) variabelen, *zoals* de bevolkingsdichtheid, het type bebouwing, de aanwezigheid van (bepaalde) winkels en voorzieningen en het gemiddelde inkomen van de inwoners van het gebied. Het systeem wordt gevoed met data over de verschillende variabelen die worden gebruikt om naar patronen te zoeken.[18] Deze data komen uit uiteenlopende bronsystemen en worden ontsloten in een datawarehouse. De (al dan niet zelflerende) algoritmen verwerken deze data tot een risicokaart op het gebied van criminaliteit; een *forecast*. Op deze kaart wordt per deelgebied aangegeven welke (categorische) kans er is dat bepaalde delicten gaan plaatsvinden: een buienradar voor criminaliteit.[19] De delicten die op deze wijze worden voorspeld, hebben vooralsnog vooral het karakter van delicten die een enigszins patroonmatig karakter (kunnen) hebben, zoals vermogensdelicten en geweld.

De 'forecast' kan vervolgens onder andere worden gebruikt om de inzet van de politie te sturen, zodat de politie zo veel mogelijk aanwezig is op plaatsen waar en tijden waarop de kans op (bepaalde) criminaliteit het hoogst is. In die zin is predictive mapping in operationele zin een doorontwikkeling van *hot spot policing*: de politie zich richt op concentraties van criminaliteit op bepaalde plaatsen en tijden (spatiotemporele patronen), maar nu ook door vooruit te kijken.[20] De beoogde sturing vindt plaats op in

15 Mali, Bronkhorst-Giesen & Den Hengst (2017) plaatsen naar mijn idee terecht vraagtekens bij de naamgeving 'predictive policing'. Het is kansberekening of, omdat het gaat over iets dat men niet wil, risicotaxatie. In het vervolg zal ik niettemin het begrip predictive policing – met de specificatie predictive mapping – gebruiken, omdat dit internationaal gangbaar is.

16 Brayne 2021; Ferguson 2017c; WRR 2016.

17 Ferguson 2017b.

18 Hoewel de systemen op een vergelijkbare manier werken, kunnen de concrete variabelen die worden gebruikt verschillen. Zo gebruikt PredPol – voor zover bij mij bekend – alleen data over het type criminaliteit, de locatie en de tijd. Het systeem gebruikt dus geen data over het gebied, zoals bevolkingsdichtheid, gemiddeld inkomen en dergelijke. Deze data worden in Nederland wel gebruikt. Zie de toelichting op het CAS.

19 Zie https://www.groene.nl/artikel/buienradar-voor-boeven (voor het laatst geraadpleegd op 7 oktober 2022).

20 Zie onder andere Ratcliffe et al. 2021; Waardenburg, Sergeeva & Huysman 2020; Waardenburg 2021.

ieder geval twee niveaus: het plannen van de capaciteit en de daadwerkelijke inzet van de capaciteit. De gedachte achter deze manier van werken is dat de aanwezigheid van de politie op deze plaatsen en tijden een preventieve werking heeft, omdat het criminelen afschrikt (*detterence*).[21] Daarnaast kan de aanwezigheid van de politie op deze plaatsen en tijden de zogenaamde heterdaadkracht vergroten: criminelen worden dan in de kraag gevat als zij hun delicten plegen (zie ook hoofdstuk 26). De systemen op het gebied van predictive mapping krijgen *veelal* feedback in de vorm van de delicten die hebben plaatsgevonden. Deze feedback wordt gebruikt om de algoritmen automatisch te verbeteren. Dit kenmerk verwijst naar het zelflerende karakter van algoritmen (zie hoofdstuk 5). Door te leren van feedback dienen de voorspellingen steeds accurater te worden, bijvoorbeeld door de weging van factoren aan te passen.

In Nederland krijgt predictive mapping op dit moment invulling door middel van het *Criminaliteit Anticipatie Systeem* (CAS). Dit systeem is – in eigen beheer[22] – ontwikkeld door de politie-eenheid Amsterdam en is, na een pilotperiode, in alle basisteams geïmplementeerd. Nederland is het eerste land dat predictive mapping op nationale schaal heeft geïmplementeerd.[23]

> **Criminaliteit Anticipatie Systeem (CAS)**[24]
> Het doel van CAS is om (kleine) gebieden aan te wijzen met een hoog risico op (bepaalde) criminaliteit in een bepaalde tijdsperiode. Dit betreft in potentie 28 verschillende delicten, waaronder woninginbraken, straatroven, overvallen, vernieling, overlast jeugd en handel in verdovende middelen. Het CAS deelt het werkgebied op in rastervakken van 125 bij 125 meter. Gebieden waarvan de kans op een incident vooraf als laag kan worden ingeschat, zoals weilanden en open water, worden verwijderd. Van de overblijvende vakjes wordt een grote hoeveelheid gegevens verzameld, zoals (geregistreerde) criminaliteitshistorie, afstand tot bekende verdachten, geografische eigenschappen (zoals afstand tot de dichtstbijzijnde snelwegoprit), soort en aantal bedrijven zoals bekend bij de politie, en demografische en sociaaleconomische gegevens van het Centraal Bureau voor de Statistiek (CBS).

21 Ferguson 2017a.

22 Dit is een (belangrijk) verschil met de systemen die in onder andere de VS worden gebruikt. Die zijn (vaker) het eigendom van commerciële bedrijven.

23 Zie de Algemene Rekenkamer (2022) en de Autoriteit Persoonsgegevens (2023) voor kritische behandelingen van het CAS. Zie ook hoofdstuk 28.

24 Deze beschrijving is vooral gebaseerd op Mali, Bronkhorst-Giesen & Den Hengst 2017; Waardenburg, Sergeeva & Huysman 2020. Er hebben in 2021 ook meerdere verzoeken in het kader van de Wet openbaarheid van bestuur plaatsgevonden. In reactie hierop heeft de politie informatie gepubliceerd die (enig) inzicht geeft in het ontwerp van het CAS.

> Van ieder vakje wordt op verschillende peilmomenten geregistreerd welke gegevens er op dat moment over de variabelen bekend zijn. Vervolgens wordt vastgelegd welke delicten in de twee weken na de peiling hebben plaatsgevonden. Per vakje wordt drie jaar historie gemeten, onderscheiden in tweewekelijkse peilmomenten. Dit resulteert in zesenzeventig peilingen per vakje. De totale set aan gegevens is dus enorm. Het CAS gaat vervolgens op zoek naar patronen: welke combinaties van variabelen zijn indicatief voor criminaliteit in de nabije toekomst? Deze patronen worden gebruikt om criminaliteit te voorspellen. Het systeem kleurt de top drie procent van de vakjes rood, oranje of geel. Vervolgens wordt bepaald wanneer het risico op een strafbaar feit het grootst is. De inzichten worden gepresenteerd op geografische kaarten: de CAS-kaarten. De CAS-kaarten worden door intelligencemedewerkers gebruikt om inzetadviezen voor de basisteams en flexteams te maken. Het doel hiervan is om politiecapaciteit in te zetten op de plaatsen en momenten die ertoe doen. Door middel van briefings en eventuele werkopdrachten wordt geprobeerd de surveillance door politieagenten te sturen.
>
> Het systeem wordt iedere week gevoed met nieuwe data. De nieuwe data worden onder andere gebruikt om de voorspelde criminaliteit te vergelijken met de criminaliteit die is geregistreerd in de periode waarop de voorspelling betrekking had. Op basis hiervan optimaliseert het systeem de algoritmen. Doordat het CAS wordt gebruikt door alle basisteams wordt er een groot beroep gedaan op de rekencapaciteit van de servers. Dit heeft er onder andere toe geleid dat de onderliggende methode die wordt gebruikt is aangepast: het CAS is begonnen als neuraal netwerk, maar later aangepast als logistische regressie. Het maken van berekeningen op basis van een neuraal netwerk kost namelijk veel tijd, terwijl men concludeerde dat een logistische regressie net zo goed zou kunnen functioneren in een derde van de tijd. Daarnaast is bij de landelijke implementatie als uitgangspunt genomen dat ieder basisteam vier delicten kan kiezen waarvoor voorspellingen worden gegenereerd. Dit (eveneens) vanwege de rekencapaciteit van de servers.[25]

Er zijn vooralsnog beperkt (experimentele) evaluatiestudies uitgevoerd naar de effecten van predictive mapping.[26] Het onderzoek dat is verricht, heeft vooral betrekking op de primaire effecten: de bijdrage van predictive mapping aan het reduceren van criminaliteit. Dit onderzoek – dat overigens heel lastig uit te voeren is en veel beperkingen kent[27] (zie ook hoofdstuk 26) – heeft geleid tot wisselende resultaten: er zijn studies waaruit positieve effecten naar voren komen en er zijn studies die geen sub-

25 Zie ook hoofdstuk 5 over het belang van rekenkracht voor AI.
26 Khalfa & Hardyns 2023.
27 Zie ook Egbert & Leese 2021.

stantieel effect van predictive mapping op de omvang van de (geregistreerde) criminaliteit hebben kunnen vaststellen.[28] Er zijn al met al nog geen overtuigende aanwijzingen dat predictive mapping bijdraagt aan het reduceren van criminaliteit.[29] De vraag die hierbij geregeld wordt overgeslagen, is of en hoe predictive mapping het optreden van de politie beïnvloedt of verandert. Dit is immers essentieel om te kunnen komen tot andere effecten in termen van criminaliteitsreductie.

Het evaluatieonderzoek in ons land laat zien dat de sturing en uitvoering van het politiewerk vooralsnog niet of nauwelijks zijn veranderd door predictive mapping.[30] Het lukt niet of nauwelijks om de capaciteitsplanning te baseren op de uitkomsten van de algoritmen[31] en daarnaast vertalen de inzichten die het CAS biedt zich vooral in surveillance inzet – in plaats van andere operationele strategieën – die vervolgens gebrekkig wordt gestuurd.[32] Kortom: de technologie wordt vooralsnog ingepast in bestaande praktijken (zie ook hoofdstuk 23). Dit is een meer algemene kritiek op deze vorm van *predictive policing*: de (verandering in) operationele strategie wordt overgeslagen.[33] Het wordt dan 'meer van hetzelfde': opdrachten aan noodhulpvoertuigen meegeven.[34] Het is in dat geval ook niet realistisch om te verwachten dat het gebruik van AI leidt tot een operationele verbetering ten opzichte van eerdere concepten.[35]

Predictive identification

Predictive identification heeft betrekking op het gebruik van AI bij risicotaxatie op individueel (persoons)niveau. In essentie gaat het hierbij om de vraag hoe groot de kans is dat een persoon (opnieuw) criminaliteit pleegt.[36] Risicotaxatie heeft internationaal gezien een lange historie in het strafrechtelijke systeem.[37] Dit begon met klinische beoordeling op het gebied van recidive: een expert die zich uitsprak over de waarschijnlijkheid dat een gedetineerde opnieuw (bepaalde) delicten gaat plegen. Sinds de jaren tachtig van de vorige eeuw zijn deze klinische beoordelingen in toenemende

28 Zie o.a. Van Brakel 2021; Ferguson 2017a; Khalfa & Hardyns 2023; Meijer & Wessels 2019; Ratcliffe et al. 2021.
29 Zie ook Terpstra & Salet 2023.
30 Deze conclusie doet overigens niet helemaal recht aan de complexiteit van en nuances in de praktijk. Zie Mali, Bronkhorst-Giesen & Den Hengst (2017), Waardenburg, Sergeeva & Huysman (2020) en Waardenburg (2021) voor een meer gedetailleerde analyse van hoe predictive mapping – in verschillende fasen (analyse, capaciteitsplanning, operatie) – doorwerkt in politieoptreden. Zie Egbert & Leese (2021) voor een zeer gedetailleerde en rijke analyse van predictive mapping in Duitsland en Zwitserland. Deze analyses laten zien hoe de uitkomsten van algoritmen (de maps) in verschillende fasen worden bewerkt en vertaald (afgestemd op de doelgroepen die ermee moeten werken), alvorens deze bij straatagenten terechtkomen.
31 Dit kan ook anders. In een experiment in Philadelphia zijn verschillende manieren van opvolging uitgetest. Vooral de (aparte) inzet van een burgerauto op basis van de voorspellingen leidde tot reductie van de vermogenscriminaliteit (Ratcliffe et al., 2021).
32 Mali, Bronkhorst-Giesen & Den Hengst 2017; zie ook Egbert & Leese 2021 voor Duitsland en Zwitserland.
33 Boba Santos 2019; Ratcliffe 2019.
34 Egbert & Leese 2021.
35 Ratcliffe 2019.
36 Zie ook Berk 2021.
37 Ávila, Hannah-Moffat & Maurutto 2021; Berk 2021; van Eijk 2021; Harcourt 2007.

mate vervangen door op statistiek gebaseerde risicotaxatie-instrumenten.[38] Deze ontwikkeling wordt in de literatuur ook wel de *actuarial turn* genoemd:

> *'They are actuarial in that they use statistical methods – rather than clinical methods – on large datasets of criminal offending rates in order to determine different levels of offending associated with a group or one of more group traits and, on the basis of those correlations, to predict the past, present, or future criminal behavior of a particular person and to administer a criminal justice outcome for that individual.'*[39]

Het gebruik van deze risicotaxatie-instrumenten heeft zich uitgebreid naar steeds meer schakels in de strafrechtketen.[40] Kenmerkend voor deze uitbreiding is *de beweging naar voren*: het begon bij de beslissing rondom (vervroegde) vrijlating en bewoog daarna naar (onder andere) het taxeren van risico's met het oog op de beslissing om iemand al dan niet in voorlopige hechtenis te nemen. Daar stopte het niet: risicotaxatie vindt ook plaats bij individuen die niet aangehouden of veroordeeld zijn, zoals bij jongeren van 12-18 jaar die nog geen strafbare feiten hebben gepleegd.

In Nederland wordt (bij mijn weten) vooralsnog vooral gebruikgemaakt van wat in de literatuur traditionele of klassieke risicotaxatie-instrumenten worden genoemd.[41] Deze instrumenten werken – vereenvoudigd toegelicht – als volgt. Op basis van wetenschappelijk onderzoek worden factoren onderscheiden die van invloed zijn op het gedrag (het delict) dat men wil voorspellen en deze factoren worden van een gewicht voorzien. De kenmerken – bijvoorbeeld geslacht en criminele historie – en omstandigheden – bijvoorbeeld gezinssituatie – van een individu worden vervolgens gebruikt om de factoren te scoren. De score per factor of variabele leidt op basis van het toegekende gewicht tot een risicoscore. Dit is dus een modelgedreven en geen datagedreven algoritme (zie hoofdstuk 4). Anders gezegd: risicotaxatie-instrumenten zijn vooralsnog vooral expertsystemen.

De politie in Nederland gebruikt diverse risicotaxatie-instrumenten die (ongeveer)[42] op de beschreven wijze werken.[43] Voorbeelden hiervan zijn ProKid (12-18-jarigen),[44]

38 Zie deze informatieve video: https://www.youtube.com/watch?v=G0OE8p-fc10 (voor het laatst geraadpleegd op 7 oktober 2022).
39 Harcourt 2007: 16.
40 Chouldevocha 2017; Van Eijk 2020; O'Neil 2016.
41 Een uitzondering is de software OXREC die door de Reclassering wordt gebruikt voor risicotaxatie op het gebied van recidive. Zie hiervoor onder andere: Hordijk & Lindsen 2023.
42 Met de nadruk op ongeveer. Er zijn verschillen in variabelen die worden gebruikt, het al dan niet toekennen van gewicht aan deze variabelen en de toepassing (geautomatiseerd op basis van enkele selecties of bijvoorbeeld aan de hand van een vragenlijst).
43 Er is een onderscheid tussen screeningsinstrumenten en risicotaxatie-instrumenten. Screening categoriseert casuïstiek; het is een vorm van triage, een eerste inschatting van het risico. Risicotaxatie verdiept casuïstiek met het oog op opvolging/behandeling. In de praktijk loopt het onderscheid tussen beide soms door elkaar, ook in benamingen.
44 Zie bijvoorbeeld Wientjes et al. 2017.

het risicotaxatie instrument huiselijk geweld (RiHG),[45] het risicotaxatie instrument geweld (RTI Geweld)[46] en het preselect recidive model voor signaleren en adviseren door de politie.[47]

Risicotaxatie-instrument Geweldplegers (RTI-Geweld)[48]
Het RTI-Geweld is een instrument om potentiële geweldplegers te identificeren en te rangschikken naar toekomstig geweldsrisico. Volgens de politie is het een instrument voor politie en partners om aan de voorkant van het probleem te komen en geweld tegen te gaan.[49] Het instrument wordt onder andere gebruikt in het kader van de persoonsgerichte aanpak (PGA) van (potentiële) plegers van high impact crimes. 'Het instrument is bedoeld voor politie, OM en de ketenpartners die betrokken zijn bij de persoonsgerichte aanpak van (potentiële) plegers van high impact crimes en die gebruik willen maken van een gevalideerd risicotaxatie-instrument om de screening en selectie van kandidaten voor deze aanpak te realiseren.'[50] Het instrument maakt gebruik van een risicofactorenmodel. Het model bestaat uit een reeks kenmerken waarvan – volgens het verantwoordingsdocument – is aangetoond dat deze samenhangen met geweldpleging. De werking van het model is gefaseerd tot stand gekomen (en wijkt daarmee ook af van de eerder gepresenteerde 'vereenvoudigde toelichting'). Op basis van een (inter)nationale literatuurstudie naar geweldpleging zijn eerst relevante factoren gedefinieerd die samenhangen met geweldpleging. Deze factoren zijn gebruikt om data uit de basisvoorziening informatie (BVI) van de politie te selecteren. Vervolgens heeft er een analyse plaatsgevonden op de factoren die (bivariaat) samenhangen met geweldspleging. Deze factoren zijn – met een bepaald gewicht – in het model opgenomen en hierbij is rekening gehouden met de beschikbaarheid van (structurele) data over deze factoren (niet alle geïdentificeerde risicofactoren zijn in het model opgenomen). De ontwerpers van het RTI-Geweld benadrukken dat het model *theorieloos* is: men weet niet of de kenmerken geweld *veroorzaken* (zie ook hoofdstuk 26), maar volstaat met de constatering dat de factoren op de een of andere manier in relatie staan tot geweldpleging. Hierbij moet worden gedacht aan

45 Zie bijvoorbeeld Römkes & Poppel 2007.
46 Zie bijvoorbeeld Rovers & Jans 2014.
47 Zie bijvoorbeeld Berends & Kempes 2015.
48 De inhoud is vooral gebaseerd op Rovers & Jans 2014. Tijdens de afronding van dit boek werd een relevant artikel door *Follow the Money* gepubliceerd. Zie www.ftm.nl/artikelen/nederlandse-politie-gebruikt-minority-report-algoritme (voor het laatst geraadpleegd op 23 augustus 2023).
49 Zie Factsheet Landelijk programma Aanpak Geweld.
50 Rovers et al. 2012: 21.

factoren als geslacht, etniciteit,[51] leeftijd eerste delict en frequentie van geweldsdelicten in de afgelopen vier jaar. Het RTI-Geweld is onderdeel van de basisvoorziening informatie (BVI) en kan geautomatiseerd en realtime risicotaxaties uitvoeren op (sub)populaties van personen. De output is een lijst van personen met bijbehorende risicoscore. Er zijn vier categorieën: laag risico, middelgroot risico, groot risico en zeer groot risico. Na een kritisch artikel over het RTI-Geweld van *Follow the Money* heeft de politie eind augustus 2023 aangegeven dat het RTI-Geweld (al dan niet definitief) uit gebruik wordt genomen, omdat er wordt getwijfeld aan het nut van het instrument.[52]

Risicotaxatie-instrumenten worden in de eerste plaats gebruikt om personen te identificeren en te prioriteren (triage): op welke individuen moeten onze inspanningen zich primair richten? De logica hierachter is zichtbaar in de veelplegeraanpak en Top X-benaderingen: de inspanningen moeten worden gericht op de individuen die zich het meest (gaan) bezighouden met criminaliteit.[53] Een volgende vraag is: welke inspanningen of interventies zouden dit dan moeten zijn? De taxatie zelf is voor het antwoord op deze vervolgvraag niet genoeg.[54] Anders gezegd: met een als 'risicovol' getaxeerd individu ben je er nog niet. Het gaat om de actie die erop volgt: hoe kan worden voorkomen dat de betreffende burger (opnieuw) delicten gaat plegen? Welke interventies zijn hiervoor nodig? Voorbeelden uit binnen- en buitenland maken duidelijk dat de insteek die hierbij wordt gekozen divers is.[55] De nadruk kan liggen op repressief optreden waarbij risicoburgers nauwlettend in de gaten worden gehouden en bijvoorbeeld veel worden gecontroleerd, maar er is ook een meer positieve aanpak op het bevorderen van beschermende factoren (opleiding, werk, zorg) mogelijk (zie ook hoofdstuk 28). Interventies door de politie en vanuit het strafrecht zijn dan een stok achter de deur, een ultimum remedium.

Er is weinig bekend over de effecten en effectiviteit van het gebruik van risicotaxatie-instrumenten door de politie in het algemeen en in Nederland in het bijzonder (zie ook hoofdstuk 26).[56] Voor zover er onderzoek is gedaan, is de accuraatheid – predictieve validiteit – onderzocht, bijvoorbeeld voor wat betreft ProKid in Nederland.[57]

51 In het verantwoordingsdocument uit 2014 is opgenomen dat etniciteit een factor is die onderdeel is van het model. Volgens de politie is deze indicator in 2017 uit het algoritme gehaald, omdat mogelijk sprake was van een beperkt maar toch nadelig effect op de interne beeldvorming voor een individu. Zie www.ftm.nl/artikelen/nederlandse-politie-gebruikt-minority-report-algoritme (voor het laatst geraadpleegd op 24 augustus 2023).

52 Zie www.ftm.nl/artikelen/politie-stopt-met-voorspellend-algoritme-geweld (voor het laatst geraadpleegd op 29 augustus 2023).

53 Hamilton 2021.

54 Hung & Yen 2020.

55 Zie Ferguson 2017a; Hamilton 2021.

56 In binnen- en buitenland is vooral onderzoek gedaan naar risicotaxatie-instrumenten op het gebied van recidive ten behoeve van de rechtspraak.

57 Wientjes et al. 2017.

Onderzoek bij de politie in het VK wijst daarnaast (indicatief) uit dat de gebruikte algoritmen soms personen naar voren brengen die politiemensen niet op hun netvlies hadden. Deze *algorithmic discovery*[58] werd door politiemensen positief gewaardeerd. Onderzoek naar de effecten van risicotaxatie-instrumenten op de persoonsgerichte aanpak en de effectiviteit daarvan is – voor zover mij bekend – niet verricht.

In zowel binnen-[59] als buitenland is er een wens om risicotaxatie verder te professionaliseren.

> *'Predictive policing in the form of individual risk assessment is likely only to broaden and solidify within organizational practices. The values are difficult to deny, particularly in the age of exponential technological transformation.'*[60]

De hiervoor bedoelde technologische transformatie gaat vooral over AI: een datagedreven vorm van actuariële risicotaxatie.[61] Het gebruik van AI bij risicotaxatie van individuen staat internationaal gezien nog in de kinderschoenen.[62] In Nederland wordt door de politie vooralsnog vooral ingezet op modelgedreven instrumenten waarbij op basis van onderzoek risicofactoren worden geïdentificeerd. Het is vermoedelijk echter een kwestie van tijd[63] voordat er in Nederland wordt meebewogen met de tendens die in met name de VS en het VK al gaande is:[64] de opkomst van *machine learning* risicotaxatie-instrumenten.[65] De primaire reden voor het gebruik van machine learning zijn de – veronderstelde dan wel voorzichtig aangetoonde – accuratere risicotaxaties.[66] Een AI-algoritme kan meer en vooral complexere verbanden leggen en patronen herkennen dan de traditionele risicotaxatie-instrumenten.[67] Daarnaast worden machine learning instrumenten gezien als een antwoord op de kritiek die op de traditionele instrumenten is geuit: de ingebakken vooroordelen. In machine learning instrumenten schuilt de belofte tot het corrigeren van deze vooroordelen.[68] Maar een belofte is nog geen praktijk. In hoofdstuk 28 kom ik hierop terug.

Naast – of eigenlijk in het verlengde van – het gebruik van machine learning instrumenten denk ik dat ook andere ontwikkelingen in de VS en het VK voorspellende

58 Marciniak 2021.
59 Zie de eerste editie van het magazine *Scherp over intelligencegestuurd politiewerk*: https://www.regioburgemeesters.nl/actueel/?id=799 (voor het laatst geraadpleegd op 7 oktober 2022). Er was of is binnen de politie een programma 'professionalisering risicotaxatie' ingericht.
60 Hamilton 2021: 70.
61 De Vries et al. 2021.
62 Hamilton 2021; Kirby & Keay 2021.
63 Zie ook De Vries et al. 2021 over risicotaxatie recidive.
64 Ávila, Hannah-Moffat & Maurutto 2021; Berk 2021; Bland 2020.
65 Hierbij wordt vaak gebruikgemaakt van een (beslisboom)methode die random forest wordt genoemd (zie Bland, 2020). Training vindt in de regel plaats op basis van supervised learning (De Vries et al., 2021). Zie hoofdstuk 5 voor deze begrippen.
66 Berk 2021; Bland 2020; Hordijk & Lindsen 2023; De Vries et al. 2021.
67 Berk 2021; Bijlsma et al. 2019; Hordijk & Lindsen 2023.
68 Ávila, Hannah-Moffat & Maurutto 2021.

waarde hebben voor wat in Nederland gaat ontstaan. Het gaat dan om twee samenhangende ontwikkelingen:[69] 1) het gebruik van meer en meer diverse data, waaronder meer justitiële gegevens en data uit open bronnen, in het bijzonder sociale media (zie ook hoofdstuk 16) en 2) inzet van algoritmen voor geautomatiseerde sociale netwerkanalyse (SNA, zie ook hoofdstuk 18). Mijn vermoeden is dat een dergelijke benadering in Nederland aantrekkingskracht heeft, omdat deze een rol kan spelen bij het voorkomen van 'jonge aanwas' en 'doorgroeiers' in de georganiseerde criminaliteit (zie hoofdstuk 7). Sociale netwerkanalyse is cruciaal, omdat het hebben van familieleden, vrienden en kennissen in de georganiseerde criminaliteit een van de belangrijkste risicofactoren voor het ingroeien in deze vorm van criminaliteit is.[70] Door middel van sociale netwerkanalyse is het mogelijk om individuen te identificeren waarbij er – vanwege hun relaties – sprake is van een hoog risico op ingroei in de georganiseerde criminaliteit. Een (enigszins) vergelijkbare benadering kan ook worden gevolgd voor risicotaxatie op het gebied van doorgroeiers.

De toekomst van predictive policing

De praktijk van predictive policing voldoet (zeker) nog niet aan de soms meeslepende teksten en video's die over dit concept te vinden zijn.

> *'Is predictive policing not as sexy as it is at times presented then? We believe it very much is. Once we strip away any superficial science-fiction layers, predictive policing offers a window into the ongoing transformation of police work along the lines of digitization, data, and algorithms.'*[71]

Predictive policing bevindt zich echter nog in een beginstadium.[72] AI ontwikkelt zich door en dit zal ook zijn weerslag hebben op de technologieën die onderdeel zijn predictive policing.[73] Krachtigere chips[74] voor meer rekenvermogen, meer databronnen en -punten,[75] meer geavanceerde analysetechnieken en functionaliteiten[76] en meer gebruik van dan wel interactie met andere apparaten (zoals smartphones)[77] zullen vermoedelijk gaan leiden tot meer, accuratere, actuelere en beter bruikbare voorspellingen c.q. risicotaxaties. Diverse onderzoekers op het gebied van technologie en politiewerk verwachten dat predictive policing uiteindelijk zal leiden tot een fundamentele transformatie in de preventie van criminaliteit (zie ook hoofdstuk 24 en 26).[78] Of deze verwachting reëel is, weet ik niet. Het realiseren van de verwachte transformatie zal in

69 Zie hiervoor Hamilton 2021.
70 De Boer, Ferwerda & Kuppens 2022.
71 Egbert & Leese 2021: 14.
72 Ferguson 2017b; Hamilton 2021; Ratcliffe 2019; Egbert & Leese 2021.
73 Berk 2021; Ferguson 2017b; Egbert & Leese 2021.
74 Berk 2021.
75 Egbert & Leese 2021; Hamilton 2021; WRR 2016.
76 Egbert & Leese 2021; Hamilton 2021.
77 Zie ook Berk 2021; Smit et al. 2016.
78 Egbert & Leese 2021; Ferguson, 2017b.

ieder geval vereisen dat er meer aandacht wordt besteed aan de opvolging van geavanceerde analyses. Deze opvolging volgt niet vanzelf uit de uitkomsten van deze analyses. 'The predictive data identifies the problem but not the solution', aldus Andrew Ferguson.[79] Zolang die opvolging of interventie – zoals surveilleren en controleren – hetzelfde is als voorheen, zal de technologie niet of beperkt bijdragen aan vernieuwing van politiewerk en de beoogde effecten hiervan (zie ook hoofdstuk 23).

Er wordt door sommige onderzoekers – in het licht van het voorgaande – gepleit voor een ontwikkeling naar *prescriptive policing*: [80] het (geautomatiseerd) aandragen van suggesties voor de opvolging. Rutger Rienks – een voormalig medewerker van de politie – vergelijkt het met een referentiedatabase die ten behoeve van de schaaksport is ontwikkeld.[81] In deze database zijn miljoenen wedstrijden opgeslagen. De data worden gebruikt om uit te rekenen welke volgende zet (vermoedelijk) het meest effectief is. Vertaald naar politiewerk: het systeem voorspelt dat er in de binnenstad 's nachts een grote kans is op auto-inbraken, de gebruiker vraagt het systeem welke interventies worden aanbevolen en hieruit komt naar voren dat surveillance te voet rond de openbare parkeervoorzieningen met focus op bepaalde automerken de meeste kans geeft op preventie en reductie.[82] Dit is een voorbeeld op basis van predictive mapping, maar ook (of misschien wel vooral) op het gebied van predictive identification is het denkbaar dat AI in de toekomst wordt gebruikt voor het aandragen van *evidence-based of -informed* interventies. In alle gevallen vereist het data over de inzet van de politie (en eventueel) partners in bepaalde situaties/contexten en de effecten van deze inzet,[83] zodat algoritmen kunnen berekenen in welke situaties welke interventies tot welke effecten leiden (en wat in die omstandigheden dus vermoedelijk de beste interventie is). Prescriptive policing is echter toekomstmuziek en de vraag is of en wanneer die muziek begint te spelen.

79 Ferguson 2017a: 87.
80 Smit et al. 2016; zie ook Mali et al. 2017; Rienks 2015.
81 Rienks 2015.
82 Zie Gigerenzer (2022: 2) over waarom de vergelijking tussen schaken en de aanpak van criminaliteit mank gaat: 'Humans are the key source of uncertainty. Imagine how much more difficult chess would be if the king could violate the rules at a whim and the queen could stomp off the board in protest after setting the rooks on fire.' Zijn stelling is: algoritmen kunnen goed voorspellen in stabiele omstandigheden, maar niet in dynamische omstandigheden, zoals bij criminaliteit.
83 Zie ook Mali et al. 2017.

Deel IV Politie

20 Politiefunctie

De politiefunctie (*policing*) heeft betrekking op het handhaven van gezamenlijke normen en regels in de samenleving.[1] De bedoeling van de politiefunctie is het gedrag van mensen in overeenstemming te houden of brengen met de normen en regels die binnen de samenleving gelden. Het is een regulatieve functie die wordt uitgeoefend door uiteenlopende partijen. Anders gezegd: er zijn in de samenleving verschillende partijen die sociale controle uitoefenen.[2] De politiefunctie heeft dus een bredere strekking dan de politie als organisatie.[3] De politie heeft tegelijkertijd wel een unieke positie binnen de bredere politiefunctie, die onder andere verband houdt met haar mogelijkheden om met dwangmiddelen te interveniëren in het domein van individuele burgers en particuliere organisaties (zie ook het volgende hoofdstuk).[4] De ontwikkelingen die in dit boek zijn beschreven, hebben naar mijn mening fundamentele gevolgen voor de politiefunctie: de politiefunctie virtualiseert en technologiseert.

Virtualisering van de politiefunctie

Het internet is een relatief nieuw domein voor handhaving van gezamenlijke normen en regels. Deel II van dit boek heeft duidelijk gemaakt dat het internet niet alleen een nieuwe gelegenheidsstructuur is voor het plegen van criminaliteit, maar ook een ruimte is waarin allerlei andere immorele gedragingen van burgers plaatsvinden en worden versterkt. In een onderzoek naar deze gedragingen concluderen onderzoekers van het Rathenau Instituut het volgende:

> *'Het internet leek altijd een domein van zelfregulering en zelfredzaamheid van de samenleving, waar de overheid geen rol had en gebruikers zichzelf wel zouden redden. Uit dit onderzoek blijkt echter dat grondrechten in het geding zijn; burgers zijn op het internet onvoldoende beschermd.*[5]

In de afgelopen jaren is steeds duidelijker geworden dat ook in de digitale ruimte een politiefunctie nodig is.[6] De traditionele, fysieke politiefunctie laat zich echter niet

1 Zie hiervoor o.a. Stol 2021; Welten et al. 2019; WRR 2021b.
2 Stol 2021; zie ook Brodeur 2010.
3 Al voor de moderne politie als overheidsorgaan in de negentiende eeuw ontstond, waren er al andere – deels private – partijen die bijdroegen aan de politiefunctie (WRR, 2021b).
4 Zie ook Niculescu-Dincă 2016.
5 Huijstee et al. 2021: 9.
6 WRR 2021b.

zomaar 'omzetten' naar een digitale variant: het is niet meer van hetzelfde.[7] Het handhaven in cyberspace heeft een heel andere dynamiek dan in de publieke ruimte in de fysieke wereld. Er is op het internet geen eenduidige rechtsorde.[8] Daarnaast zijn de bouwstenen van het internet – van de onderzeese kabels tot de apps – primair privaat bezit (zie ook hoofdstuk 6). Sociale mediaplatformen kunnen weliswaar worden beschouwd als *de facto* publieke ruimten waar onder andere burgers hun meningen ventileren, politici hun standpunten publiekelijk maken en academici hun onderzoeksresultaten verspreiden, maar het zijn bedrijven die deze ruimten beheren.[9] De politiefunctie op het internet wordt in veel gevallen allereerst uitgeoefend door private partijen die sociale normen op hun digitale platformen afdwingen door degenen die deze normen overtreden te sanctioneren.[10] In die zin is er als gevolg van digitalisering ook sprake van privatisering van de politiefunctie.[11]

Het gegeven dat private partijen veelal de eerst aangewezen partijen zijn om sociale controle op het internet uit te oefenen wil niet zeggen dat zij dit ook doen. De grote spelers in de digitale wereld – zoals Meta – zijn primair gericht op gedragsbeïnvloeding van burgers met het oog op commerciële doeleinden.[12] Zij hebben een economisch model ontwikkeld waarin het op grote schaal verzamelen en commercieel benutten van persoonlijke data van gebruikers centraal staat. Dit is wat Shoshana Zuboff *surveillance capitalism* noemt.[13] De private bedrijven die de online ruimten beheren, hebben uitsluitend belang bij het uitoefenen van sociale controle voor zover dit nodig is om hun reputatie en – in het verlengde daarvan – machtspositie te beschermen. De machtspositie van deze poortwachters is vooralsnog echter zo groot dat publieke waarden worden verdrongen door de commerciële logica.[14] Wat resulteert, is een cyberspace die *underpoliced* is.[15] Burgers voelen zich online minder beschermd dan offline: zij ervaren cyberspace als grenzelozer.[16] Het gebrek aan handhaving van de digitale orde is problematisch, omdat een rechtsstaat niet alleen een rechtvaardig stelsel van formele normen en waarden is, maar ook een systeem dat erin dient te slagen om dit stelsel geloofwaardig en herkenbaar te handhaven. In een wereld die verder digitaliseert, wordt dit een steeds grotere opgave.[17] Dit roept de vraag op wat de rol is van de politie in het beschermen en begrenzen op het internet.

7 Idem.
8 Boutellier 2020.
9 WRR 2021b.
10 Idem.
11 Waar de politiefunctie in het fysieke domein vooral wordt uitgeoefend door uiteenlopende publieke partijen – gemeentelijke handhavers, boswachters, talrijke specifieke toezichthouders et cetera – is dit in het digitale domein dus niet het geval.
12 Zie ook Verhoeven 2023.
13 Zuboff 2019.
14 Zie ook Morozov 2013.
15 WRR 2021b.
16 Huijstee et al. 2021.
17 Zouridis 2019.

Voor delicten die zijn opgenomen in het Wetboek van Strafrecht is de politie in principe aan zet met opsporingsinspanningen. De omvang van deze opgave neemt bij voortduring toe, omdat steeds meer (immorele) online gedragingen van burgers strafbaar worden gesteld. Hierbij kan onder andere worden gedacht aan de strafbaarheidstelling van doxing – het openbaar maken van persoonsgegevens om iemand te intimideren – per 1 januari 2024. Iedere strafbaarheidsstelling resulteert in een – soms complexe – handhavingsopgave. Voor gedragingen die niet zijn opgenomen in het Wetboek van Strafrecht is er sprake van een andere situatie. Hierbij doet zich in de eerste plaats de vraag voor wat de norm zou moeten zijn: '…what remains impossible to achieve is a consensus on exactly what should and should not be allowed', aldus Matthew David in zijn boek *Networked crime*.[18] Naarmate de norm minder duidelijk en afdwingbaar is, wordt de positiebepaling van de politie in handhaving van de digitale orde ingewikkelder.[19] Het gaat dan om allerlei immorele gedragingen op het internet die burgers het gevoel geven onbeschermd te zijn, zoals vormen van online haat, online pesten en online vigilantisme. In dit schemerdomein is de overheid in het algemeen en de politie in het bijzonder vooralsnog meer handelingsverlegen dan in het domein van de digitale criminaliteit.[20] Ook in dit schemerdomein zal het aantal onwenselijke fenomenen eerder toe- dan afnemen. Generatieve AI zal hierin een belangrijke factor zijn.

Wanneer de gevolgen van dergelijke immorele en schadelijke gedragingen merkbaar zijn in de fysieke wereld, zoals in geval van online aangejaagde ordeverstoringen of conflicten tussen drillrap groepen, dan ligt een rol voor de politie vanzelfsprekend voor de hand. Maar wat te doen wanneer de (directe) gevolgen van schadelijk en immoreel gedrag zich beperken tot cyberspace? Het Rathenau Instituut stelt dat bedrijven, maatschappelijke organisaties en burgers een actieve overheid nodig hebben om schadelijk en immoreel gedrag online tegen te gaan en sociaal wenselijk gedrag online te bevorderen.[21] In het verlengde hiervan pleiten zij voor meer zichtbaarheid van de politie online, zodat gebruikers eraan worden herinnerd dat het internet geen wetteloze omgeving is. De roep om meer online zichtbaarheid van de politie zal met de opkomst van de metaverse vermoedelijk verder toenemen (zie hoofdstuk 9).[22] In een verkenning van het innovatielab van Europol naar de metaverse wordt een – wat mij

18 David 2023: 191.
19 Boutellier 2020.
20 Huijstee et al. 2021.
21 Idem.
22 In *Het Tijdschrift voor de Politie* vraagt het Rathenau Instituut welke rol de politie in Nederland voor zichzelf in de metaverse ziet (zie Roolvink, Kuijvenhoven & Huijstee, 2022). In Amen in de Verenigde Arabische Emiraten is de politie aan het experimenteren met aanwezigheid van de politie in de metaverse. Zeven politieagenten zijn getraind in het gebruik van de technologie, waaronder de VR headsets. Zie https://www.thenationalnews.com/uae/2022/06/06/uae-police-set-up-metaverse-service-to-help-the-public/ (voor het laatst geraadpleegd op 1 augustus 2022). In oktober 2022 opende Interpol diens eigen metaverse ten behoeve van trainingen. Een bijkomend doel is dat politiemensen wereldwijd via de Interpol Metaverse ervaring kunnen opdoen met aanwezigheid in en het werken in de metaverse. Om de metaverse te begrijpen, moeten we het ervaren, zo luidt het uitgangspunt. Zie https://www.interpol.int/News-and-Events/News/2022/INTERPOL-launches-first-global-police-Metaverse (voor het laatst geraadpleegd op 24 oktober 2022).

betreft – helder uitgangspunt geformuleerd: 'The police needs to be where the people are.'[23] Ook de politie in Nederland lijkt een dergelijk uitgangspunt te hanteren: de politie is daar aanwezig waar burgers zijn en interacteren en dat is dus nadrukkelijk en in toenemende mate (ook) op het internet.[24]

De vraag is echter wat de praktische implicaties van dit uitgangspunt zouden moeten zijn. Hans Boutellier stelt dat de politie haar normatieve gezag ook digitaal moet laten gelden, maar voegt hier direct aan toe dat de politie zich niet moet laten gek maken.[25] Er kan volgens hem geen digitale agent op het internet zijn die hetzelfde doet als de wijkagent in de fysieke wereld. Een dergelijke stellingname kan ik mij voorstellen, want dit zou ertoe (kunnen) leiden dat er min of meer een nieuwe politie bij komt.[26] De vraag wat het wel zou moeten zijn, is daarmee echter nog niet beantwoord. De politie in Nederland is al enige tijd bezig om de brede vraag te beantwoorden wat haar rol en positie op het internet – nu en in de toekomst – moet zijn.[27] In een artikel van twee strategie-adviseurs van de politie wordt gesteld dat het motto 'niet meer, maar anders' hierbij leidend moet zijn. Hoe aantrekkelijk dit motto ook mag klinken, het lijkt mij lastig in de praktijk te brengen. Een uitvoerende politiefunctionaris die op straat meldingen behandelt en met burgers in contact is, is simpelweg niet bezig met sociale controle online. Dat de fysieke en digitale samenleving met elkaar zijn verweven, betekent niet dat de politie met dezelfde inspanningen in beide domeinen sociale controle kan uitoefenen. De adviseurs stellen naar mijn idee terecht dat er nieuwe operationele concepten of ideeën nodig zijn, maar het artikel maakt ook duidelijk dat deze nog niet zijn gevonden. Er zijn, mede op basis van de ervaringen met de aanpak van digitale criminaliteit, wel uitgangspunten te formuleren. Ik beperk me tot twee uitgangspunten die ik relevant acht. Het eerste uitgangspunt is dat (internationale) publiek-private samenwerking nodig is, omdat de publieke politie uiteindelijk een beperkte speler is in de (internationale)[28] politiefunctie op het internet en begrensde mogelijkheden heeft.[29] Het tweede uitgangspunt is dat het gebruik van digitale technologie in het handhaven van de digitale orde cruciaal is, omdat dit de enige manier is om met relatief beperkte capaciteit op relatief grote schaal te kunnen opereren. Dit brengt me bij het tweede thema van dit hoofdstuk: technologisering van de politiefunctie.

23 Dit baseer ik op een LinkedIN-post over deze verkenning (zie Europol, 2022b).
24 Zie Van Wijngaarden & Schiffelers 2023.
25 Boutellier 2020.
26 Wellicht ten overvloede: een dergelijke rolinvulling gaat veel verder dan wat een digitaal wijkagent nu doet (zie ook Boelens & Landman, 2021).
27 Van Wijngaarden & Schiffelers 2023.
28 Boutellier (2020) en de WRR (2021b) wijzen erop dat het perspectief op de politiefunctie en de rol van de politie niet los kan worden gezien van regulering van het internet in het algemeen en de grote platformen in het bijzonder. Dit vraagstuk van *internetgovernance* is een internationaal vraagstuk. Zie voor meer verdieping onder andere de WRR (2015).
29 Wall 2007.

Technologisering van de politiefunctie

Digitalisering heeft niet alleen geleid tot een nieuw domein waarin de politiefunctie wordt uitgeoefend, maar heeft ook tot gevolg dat er verandering optreedt in de wijze waarop de politiefunctie wordt uitgeoefend. Dit komt doordat digitalisering nieuwe mogelijkheden biedt in het kader van handhaving van de rechtsorde en sociale controle.[30] Deze mogelijkheden worden – zowel offline als online – in toenemende mate benut. Dit leidt tot technologisering van de politiefunctie: het uitoefenen van (aspecten van) sociale controle *door technologie*. Technologie wordt dan een actor in het beïnvloeden van het gedrag van burgers teneinde dit gedrag in overeenstemming te brengen met de normen en regels die in de samenleving gelden.

De technologisering van de politiefunctie is een ontwikkeling die zich over de volle breedte van deze functie voltrekt. Dit boek gaat vooral over de politie, maar er zijn ook partijen 'boven', 'naast' en 'onder' de politie die bijdragen aan de technologisering van de politiefunctie.[31] 'Boven' de politie gaat het om organisaties en initiatieven die een internationaal karakter hebben. Hierbij kan onder andere worden gedacht aan Europol, die de (big) data uitwisseling tussen landen faciliteert. 'Naast' de politie gaat het om private organisaties en overheidsorganisaties die door middel van technologie sociale controle uitoefenen. Hierbij kan onder andere worden gedacht aan lokale overheden en allerlei uitvoeringsorganisaties – waaronder bijzondere opsporingsdiensten – die technologie benutten voor hun handhavingstaak. 'Onder' de politie gaat het om burgers die in hun eigen leefomgeving technologie inzetten om ervoor te zorgen dat anderen zich gedragen in overeenstemming met de normen en regels die in de samenleving gelden. Hierbij kan onder andere worden gedacht aan burgers die slimme camera's of deurbellen gebruiken in de verwachting daarmee meer controle op hun leefomgeving te kunnen uitoefenen (en hierbij al dan niet samenwerken met de politie).[32]

In het vervolg van dit hoofdstuk richt ik me vooral op de inzet van technologie ten behoeve van de politiefunctie die wordt uitgeoefend door de overheid (dus 'naast' en 'met' de politie). In dit kader is de *slimme stad* een van de meest relevante concepten waarin de technologisering van de politiefunctie concreet gestalte krijgt. De slimme stad is een stad waarbij technologie – in het bijzonder de IoT (zie hoofdstuk 3) – wordt gebruikt om de stad te beheren en te besturen.[33] In dat kader worden (persoons)gegevens over of in de openbare ruimte verzameld en verwerkt door de inzet van sensoren en andere technologische toepassingen. Dit betreft onder andere de inzet van uiteenlopende camera's, wifi- en bluetoothtracking en allerlei andere sensoren die data verza-

30 Idem.

31 Zie hiervoor Schuilenburg (2023) die er overigens op wijst dat in de praktijk het onderscheid tussen deze categorieën partijen in elkaar overloopt.

32 Zie ook de voetnoten in hoofdstuk 14 over slimme camera's.

33 In Nederland zijn er vooralsnog grote verschillen tussen gemeenten voor wat betreft de inzet van smart city-toepassingen (zie AP, 2021). De ambitie om een slimme stad te ontwikkelen, wordt breed gedeeld. Zie hiervoor onder andere de website van de Vereniging van Nederlandse Gemeenten (VNG).

melen over de stad en diens burgers.[34] Kenmerkend is dat de sensoren met elkaar een netwerk vormen waarin data worden verzameld en geanalyseerd. De slimme stad is meer dan een digitale weergave van fysieke processen die in de stad plaatsvinden.[35] Er wordt ook sociale controle uitgeoefend.

> *'Technology is reconfiguring urban life. In the "smart city", data and information do more than just represent urban processes – they intervene in them.'*[36]

De meest vergaande vorm van sociale controle in de slimme stad of slimme samenleving treffen we aan in China.[37] De steden hangen vol met camera's – uitgerust met gezichtsherkenning – en andere sensoren. Er is ook sprake van grootschalige online surveillance. De sociale controle wordt in de eerste plaats uitgeoefend doordat burgers zich bekeken (kunnen) voelen en op basis daarvan hun gedrag aanpassen. Daarnaast wordt geëxperimenteerd met sociaalmanagementsystemen, die ook wel sociaalkredietsystemen worden genoemd. Dit zijn systemen die zijn bedoeld om het gedrag van individuele burgers te monitoren, beoordelen en bij te sturen. Burgers die zich op de een of andere manier misdragen ondervinden daar nadelen van, bijvoorbeeld doordat zij geen gebruik kunnen maken van bepaalde voorzieningen of publiekelijk aan de 'schandpaal worden genageld'. Een voorbeeld van de eerste variant is een nationale lijst van personen die in gebreke zijn gebleven nadat hen door middel van een rechterlijke uitspraak een boete is opgelegd. Mensen op die lijst mogen onder andere niet in hotels verblijven, want ze hebben eerst iets anders te betalen. Een voorbeeld van de tweede variant is een experiment waarin voetgangers die regelmatig door rood licht lopen door middel van gezichtsherkenning worden geïdentificeerd en met naam en toenaam op een publicatiebord verschijnen. Naast deze varianten van sociale controle zijn er ook (nog) meer vergaande vormen, onder andere in de Xinjiang regio waar Oeigoeren – met gebruik van geavanceerde technologieën – systematisch worden onderdrukt.[38]

Ik gebruik China hier slechts om te verhelderen hoe de uitoefening van sociale controle door technologie eruitziet. Nederland is geen China, maar dit neemt niet weg dat er overeenkomsten zijn.[39] Ook in Nederland vindt – door middel van onder andere slimme steden en geautomatiseerde online monitoring – technologisering van de politiefunctie plaats. Zo is er aan de kust in Scheveningen een living lab in het kader van de

34 Zie AP 2021.
35 Ter toelichting: een slimme stad bestaat uit een netwerk van sensoren die met elkaar min of meer een digitale kopie (*digital twin*) van de stad vormen. Deze digitale kopie maakt het onder andere mogelijk om over allerlei activiteiten in de stad data te verzamelen die vervolgens kunnen worden gebruikt voor het beheren en besturen van de stad.
36 Shapiro 2020: 1.
37 Cain 2021; Gerritsen et al. 2020.
38 Idem.
39 Buitenweg 2021; Gerritsen et al. 2020; Rathenau Instituut 2021.

slimme stad.[40] De politie, gemeente Den Haag en andere partners werken in deze leeromgeving samen aan digitale innovaties in de buitenruimte ten behoeve van (onder andere) leefbaarheid en veiligheid. Een van de toepassingen die wordt ontwikkeld, is een 'Crowd Safety Manager'. Dit is een tool die op basis van data uit uiteenlopende bronnen de drukte voorspelt en passende maatregelen voorstelt. Er wordt gebruik gemaakt van camera's die beelden – met behulp van een algoritme – automatisch omzetten in aantallen aanwezige mensen en groepsvorming detecteren. Daarnaast worden sensoren ingezet die geluiden registreren. Een algoritme zet de geluiden om in een spectrogram op basis van waarvan geluiden worden gecategoriseerd, bijvoorbeeld in muziek of verkeer. Kortom: in de slimme stad worden burgers door technologie gemonitord gericht op het bijsturen van hun gedrag ten behoeve van (onder andere) de leefbaarheid en veiligheid. Onderdelen van sociale controle worden hierdoor in toenemende mate uitgeoefend door technologie.

> *'… as cities become 'smarter', they increasingly embed policing itself into the urban infrastructure. Policing is inherent to the smart city.'*[41]

De Crowd Safety Manager wordt ontwikkeld door een consortium waarin de politie samenwerkt met private en publieke partijen. De ontwikkeling is onderdeel van de zogenaamde 'Impact Coalitie Safety & Security voor Smart Society'. Dit is een landelijke samenwerking tussen onder andere de politie en de gemeenten Den Haag, Amsterdam, Apeldoorn, Almere, Eindhoven, de Vereniging Nederlandse Gemeenten (VNG) en de Security Delta.[42] In het samenwerkingsverband worden geslaagde digitale toepassingen die bijdragen aan een veilige stad met elkaar gedeeld. Naast de Crowd Safety Manager gaat het dan onder andere om vormen van gezichtsherkenning waarmee is geëxperimenteerd in de omgeving van de Johan Cruijff Arena in Amsterdam (zie ook hoofdstuk 14).[43] De ontwikkeling naar slimme steden – of breder: de slimme samenleving – bevindt zich in Nederland in een beginstadium en zal zich de komende jaren vermoedelijk verder ontwikkelen.[44]

> **Een magisch schild om de stad**[45]
> In Europees verband ligt er een nieuw plan. Nieuwe auto's in Europa moeten zijn uitgerust met een ISA: Intelligent Speed Assistance. Dit is een digitale snelheidsbegrenzer. De EU legt dit als verplichting op aan autofabrikanten. De ISA kan door wegbeheerders worden benut door via GPS virtuele zones

40 Zie hiervoor onder andere de brief van wethouder Bruines van Den Haag over de voortgang van het Living Lab Scheveningen aan de gemeenteraad van 31 mei 2022.
41 Joh 2019: 178.
42 https://vng.nl/nieuws/gemeenten-en-politie-werken-samen-aan-smart-society (voor het laatst geraadpleegd op 16 augustus 2022). De Security Delta is een cluster van 275 overheden, kennisinstellingen en bedrijven die samenwerken aan innovatieve veiligheidsoplossingen.
43 Zie Van Vliet et al. (2019) voor een overzicht van kansen van de 'smart city' voor stedelijke veiligheid.
44 Zie ook Ferguson 2022b voor de VS.
45 Zie Februari 2023.

> in te stellen waarbinnen de assistent de auto simpelweg niet harder laat rijden dan in die zone is toegestaan. Deze zone kan worden bepaald op basis van onder andere voertuigtype (zodat bijvoorbeeld hulpverleners er geen last van hebben), plaats, tijd, weeromstandigheden, drukte of wegwerkzaamheden. In januari 2022 was in media te lezen dat de vier grote steden bij de Tweede Kamer hebben gepleit voor het benutten van de techniek voor het begrenzen van de snelheid van auto's in de stad op maximaal 30 kilometer per uur.[46] Maar er is meer mogelijk, zo legt een verkeersdeskundige uit. 'Op sommige drukke verkeerskruispunten – waar bijvoorbeeld trams, fietsers en auto's samenkomen – zijn drempels of verkeerslichten geen optie. Op dat soort plaatsen heb je deze nieuwe techniek echt nodig om de snelheid omlaag te brengen'.[47] Of: rond een school kun je een 'magisch schild' aanleggen tijdens de haal- en brengtijden van kinderen, zodat er daar op die momenten alleen stapvoets kan worden gereden.[48]

Het voorbeeld van het 'magisch schild' maakt duidelijk hoe in de slimme samenleving de technologisering van de politiefunctie – het beïnvloeden dan wel afdwingen van gedrag van burgers door technologie – voortschrijdt. Net als bij virtualisering geldt dat deze ontwikkeling onvermijdelijk gepaard gaat met privatisering van de politiefunctie, omdat een deel van de technologie die wordt gebruikt, is ontwikkeld en wordt beheerd door bedrijven.[49] Het is daarnaast van belang te benadrukken dat de technologisering van de politiefunctie van invloed is op hoe de rechtsstaat zich ontwikkelt. Computercode vervult namelijk in toenemende mate een eigenstandige regulerende functie in de samenleving.[50] Deze regulerende functie bestaat naast wetgeving, maar komt niet op dezelfde democratische wijze tot stand. In die zin verandert de normatieve orde – het recht – in de samenleving.[51] De technologisering van de politiefunctie vraagt daarom alertheid van iedereen die waarde hecht aan hoe de rechtsstaat zich ontwikkelt.[52]

Binnen de technologisering van de politiefunctie is er sprake van *technologisering van politiewerk*. In het derde deel van dit boek zijn hier vele voorbeelden van gegeven. De rode draad in de ontwikkeling is – naar mijn idee – dat de relatie tussen technologie en politiewerk aan het veranderen is. De digitaliseringsgolf die in de derde industriële revolutie is ontstaan, heeft ertoe geleid dat de politie informatie- en communicatietechnologie is gaan gebruiken ter ondersteuning van het politiewerk.[53] In de over-

46 https://nos.nl/nieuwsuur/artikel/2414102-maximaal-30-kilometer-per-uur-door-magisch-schild (voor het laatst geraadpleegd op 23 februari 2023).
47 Idem.
48 https://decorrespondent.nl/12566/hoe-je-30-kilometer-per-uur-in-amsterdam-handhaaft-een-magisch-schild-op-de-weg-is-een-optie (voor het laatst geraadpleegd op 23 februari 2023).
49 Februari 2023; Joh 2019.
50 Diver 2022.
51 Gebaeerd op: Februari 2023.
52 Februari 2023; Diver 2022.
53 Stol 1996.

gangsfase van de derde naar de vierde industriële revolutie wordt steeds duidelijker dat de secundaire functie van technologie verandert in een – op onderdelen – primaire functie. Dit komt doordat technologie processen van betekenisgeving in toenemende mate van politiemensen overneemt en zich zo beweegt van de randen naar de kern van het politiewerk. In de volgende hoofdstukken ga ik hier nader op in.

21 Politievermogens

De essentie van wat de politie is en doet, kan op verschillende manieren worden gedefinieerd en geoperationaliseerd, zoals in kerntaken of identiteitskenmerken. In dit hoofdstuk maak ik gebruik van een uitwerking in vermogens. Een vermogen is een combinatie van mensen, middelen en methoden die de politie voor de uitvoering van haar taken inzet.[1] Ik maak onderscheid tussen vier vermogens en gebruik hierbij het menselijk lichaam als metafoor: de ogen, het brein, de tanden en het hart van de politie. Deze vermogens gebruik ik om de impact van technologiegebruik te duiden.

De ogen van de politie

In de samenleving speelt zich een voortdurende stroom van activiteiten en gebeurtenissen af: burgers zijn offline en/of online met iets bezig. Voor de politie is deze stroom van activiteiten van belang vanuit het perspectief van de orde die zij wordt geacht te handhaven.[2] Simpel gezegd: burgers kunnen met hun activiteiten inbreuk maken op de openbare of strafrechtelijke orde in de samenleving en het is dan aan (onder andere) de politie om op te treden. Dit impliceert dat de politie voor de opgave staat om deze activiteiten waar te nemen.[3] Maurice Punch noemde dit in zijn studie naar politiewerk het 'scannen van de maatschappelijke horizon'.[4] Peter K. Manning spreekt over het 'schaduwen' van burgers'.[5] De ogen van de politie gaan daarover: het waarnemingsvermogen van de politie. Het doel is niet zozeer het 'zien' van de burger als mens (relationeel), maar om het 'bekijken' ervan als object.[6]

> *'Het zichtbaar maken van activiteiten van mensen is daarbij een centrale opgave voor de politie. Surveillance in de brede betekenis van het woord, heeft daarop betrekking.[7] In dat opzicht geldt niet zozeer dat de politie zelf zichtbaar moet zijn, maar dat de politie gedrag van geïndividualiseerde burgers zichtbaar moet maken, het liefst goedkoop en onomstreden.'*[8]

1 Zie bijvoorbeeld Davies 2002.
2 Landman 2015.
3 Stol 1996.
4 Punch 1983.
5 Manning 2010.
6 Zie voor het onderscheid tussen 'zien' en 'bekijken' ook Nap 2014.
7 Surveillance komt onder andere uit het Latijns en betekent het in de gaten houden van (hen) beneden. Zie ook Marx (2016) en Lyon (2018).
8 Stol 1996: 20.

Door middel van haar waarnemingen vergaart de politie kennis over burgers met het oog op het handhaven van de orde en sociale controle. Ericson en Haggerty spreken over '… the routine production of knowledge of populations useful for their administration.'[9] Het waarnemingsvermogen van de politie is niet alleen bedoeld om de gang van zaken te observeren en kennis te produceren, maar ook om burgers te disciplineren.[10] Simpel geformuleerd: wie weet dat hij in de gaten wordt gehouden, past daar in de regel diens gedrag (enigszins) op aan (zie ook hoofdstuk 20). Bijvoorbeeld: je rijdt te hard op een punt waarvan je weet dat de politie er vaak staat te controleren en gaat daarom minder hard rijden. Het waarnemingsvermogen van de politie leidt in potentie dus tot preventieve effecten, omdat het een afschrikkende werking kan hebben.

Het waarnemingsvermogen van de politie wordt van oudsher bepaald door politiemensen die observeren. Door een toenemend aantal sensoren wordt dit waarnemingsvermogen versterkt en deels ook geautomatiseerd. In hoofdstuk 17 werd de aanhouding van de verdachten van de moord op Peter R. de Vries behandeld. De ANPR-camera heeft hierbij een belangrijke rol gespeeld (zie ook hoofdstuk 14). De chef van het RTIC gaf hierbij de volgende toelichting: 'Tien tot vijftien jaar geleden werden verdachten in soortgelijke situaties minder snel gepakt. Toen moesten de lokale eenheden op een viaduct boven de snelweg of op de vluchtstrook worden gepositioneerd om te zien of de verdachten voorbijkwamen.'[11] Dit voorbeeld maakt duidelijk hoe sensoren politiemensen op onderdelen vervangen. Het gaat in dit voorbeeld om een enkele sensor langs een snelweg die een signaal heeft doorgegeven. Deze afzonderlijke sensoren worden in toenemende mate onderdeel van een netwerk of systeem van sensoren waarmee de gang van zaken in de fysieke wereld en deels ook digitale wereld wordt waargenomen (zie ook hoofdstuk 17 en 20). Dit zorgt voor een exponentiële uitbreiding van het waarnemingsvermogen van de politie.[12] Het waarnemingsvermogen van de politie raakt in toenemende mate 'ontkoppeld' van het waarnemingsvermogen van politiemensen.[13] Hierdoor worden traditionele beperkingen in het waarnemingsvermogen overwonnen en verandert dit vermogen van de politie fundamenteel van karakter.[14] Dit biedt potentie met het oog op effectiviteit en efficiëntie (zie hoofdstuk 26), maar gaat ook gepaard met bedreiging van publieke waarden, waaronder het recht om door de overheid met rust gelaten te worden (zie hoofdstuk 27).

9 Ericson & Haggerty 1997: 450.
10 Foucault 1989.
11 https://www.nrc.nl/nieuws/2021/07/16/hoe-verdachten-aanslag-peter-r-de-vries-zo-snel-konden-worden-gearresteerd (voor het laatst geraadpleegd op 16 augustus 2021).
12 Brayne 2021; Ferguson 2020b; Simmons 2019.
13 Ferguson 2022.
14 Ik citeer Ferguson (2022: 29), omdat hij het zo mooi formuleert: 'No one was trying to add a dataset or other information to a beeper, pen register, or cassette tape. Tools were tools. But when tools become systems and systems become networked, the capabilities change… Digital surveillance technology is different, not simply because of what it is, but also because of what it can become.' Zie ook hoofdstuk 27 voor de risico's hiervan.

Het brein van de politie

Politiewerk is ook informatiewerk.[15] De politie staat bij voortduring voor de opgave om gegevens te verwerken en daar conclusies aan te verbinden. Dit doet zich voor in alle vormen van politiewerk: in het straatwerk wanneer moet worden ingeschat of er sprake is van een verdachte situatie, in het recherchewerk wanneer gegevens moeten worden geanalyseerd om strafbare feiten te reconstrueren en in het intelligencewerk waarin grote hoeveelheden gegevens worden gebruikt om sturingsinformatie te genereren en probleemgerichtheid te bevorderen. Bij het verwerken van gegevens doet de politie een beroep op haar brein: het cognitieve vermogen.

Ook voor het cognitieve vermogen van de politie geldt dat dit vermogen van oudsher wordt bepaald door politiemensen die gegevens – al dan niet met behulp van een computer – verwerken en tot uitkomsten komen in bijvoorbeeld informatierapporten en processen-verbaal. Het gebruik van opkomende technologieën in het politiewerk heeft veel invloed op het brein van de politie. Het vorige deel van dit boek heeft laten zien dat er in het politiewerk gebruik wordt gemaakt van een groeiend aantal algoritmen waarmee betekenis wordt gegeven aan allerlei data in het kader van vrijwel alle politietaken. Deze algoritmen worden ingezet voor diverse doeleinden: reconstrueren, realtime observeren en voorspellen.[16] Het gebruik van algoritmen binnen de politie leidt tot een exponentiële uitbreiding van het cognitieve vermogen van de politie. De gegevensverwerking in de politieorganisatie wordt niet meer beperkt tot de cognitieve vermogens van politiemensen.[17]

De uitbreiding of versterking van het brein is van een recentere datum dan die van de ogen van de politie en ontwikkelt zich snel. Vaardigheden of talenten die voorheen werden beschouwd als menselijke vaardigheden – zoals het herkennen van verdachte situaties en verbanden leggen tussen informatie in een opsporingsonderzoek – worden in toenemende mate ook uitgevoerd door 'slimme systemen'.[18] Het gaat dus niet alleen om het versterken van het cognitieve vermogen van politiemensen, maar ook om het – op onderdelen – automatiseren ervan. In sommige gevallen worden taken die van oudsher handmatig werden uitgevoerd overgenomen door software. Er is echter vaker sprake van een vorm van gegevensverwerking die voorheen niet plaatsvond, omdat deze simpelweg niet door politiemensen kon worden uitgevoerd (en dan kan er in letterlijke zin geen sprake zijn van overnemen).

> *'… the resulting collection of searchable and predictive data is something largely impossible for humans to use and only available because of powerful computer and analytical capacities.'*[19]

15 Bacon 2016; Ericson & Haggerty 1997; Manning 1980.
16 Zie ook Schuilenburg & Soudijn 2021.
17 Ariel 2019.
18 Joh 2018b.
19 Ferguson 2022: 26.

Een relevante vraag is hoe het automatiseren van het cognitieve vermogen van politiemensen zich in de toekomst gaat ontwikkelen. In het hoofdstuk over politievakmanschap kom ik hierop terug.

De tanden van de politie
Volgens de Britse politiesocioloog Egon Bittner hebben de situaties in de samenleving waarin er behoefte is aan de politie met elkaar gemeen dat zich iets voordoet dat door iemand als onwenselijk wordt ervaren. Er is vervolgens 'iemand' nodig die ervoor zorgt dat daaraan snel een einde komt.[20] Dit is veelal de politie. Waarom de politie? Omdat de politie als unieke competentie heeft dat zij te allen tijde, en tegen de wil van burgers in, dwang kan gebruiken (zie ook hoofdstuk 20). De politie reageert op allerlei situaties waarin het gebruik van dwang – van verbale dwang tot het gebruik van wapens – nodig *zou kunnen zijn*. De politie heeft hierbij doorzettingsmacht: als alle andere oplossingen tekortschieten, dan is er uiteindelijk nog altijd de harde hand of sterke arm van de politie.[21]

Bij het uitoefenen van dwang doet de politie een beroep op haar tanden: het fysieke vermogen. Dit vermogen gaat in essentie niet om de feitelijke toepassing van dwang – in wat voor vorm dan ook – maar om het idee dat het kan worden toegepast.[22] Wanneer burgers geloven dat de dreiging van dwang reëel is, kan deze dreiging als zodanig voldoende zijn om daadwerkelijke dwang te laten rusten.[23] Deze afschrikkende werking van de tanden van de politie neemt niet weg dat politiemensen met regelmaat in situaties terechtkomen waarin daadwerkelijk enige vorm van dwang moet worden toegepast. Dit is niet zonder risico. Politiemensen drukken dit vaak uit met de zin: waar anderen een stap terug doen, stappen wij naar voren.[24]

De tanden van de politie worden in veel mindere mate beïnvloed door opkomende technologie dan de ogen en het brein van de politie. Voor zover er van invloed sprake is, gaat het om het versterken van het fysieke vermogen. Een voorbeeld hiervan is de invoering van het stroomstootwapen.[25] Van automatisering van het fysieke vermogen is (vooralsnog) geen sprake. Bij de introductie van robothond Spot werd door de politie benadrukt dat deze geen geweld zal uitoefenen en ook niet wordt ingezet voor bijvoorbeeld aanhoudingen. De robothond wordt uitsluitend ingezet voor verkenningen

20 Bittner 1970: 132.
21 Cachet 2019.
22 Het zijn de tanden van de politie die de dreiging van dwang een reëel karakter kan geven (zie Van Reenen, 2010). Anders geformuleerd: een politie die burgers geen enkele angst kan inboezemen, schiet als dreigingssysteem tekort.
23 Van Reenen 2010.
24 Zie bijvoorbeeld https://www.politie.nl/blogs/00-korpsmedia/blog-stap-naar-vo.html (voor het laatst geraadpleegd op 4 mei 2021).
25 Onderzoek naar de pilots met het stroomstootwapen in de basisteams laat zien hoe de dreiging van geweld voldoende kan zijn om daadwerkelijk geweld te laten rusten. In twee derde van de situaties was het dreigen met gebruik van het stroomstootwapen voldoende om medewerking van de betreffende burger te krijgen (zie Adang, Mali & Vermeulen, 2022).

(zie hoofdstuk 15). In algemene zin moet worden opgemerkt dat (verdere) inzet van technologie voor geweldsuitoefening in de toekomst niet is uit te sluiten. Hoewel politie en Defensie niet (volledig) vergelijkbaar zijn, geeft de discussie over drones met bewapening wel weer hoe deze in de regel verloopt: de inzet van bewapende drones lag jarenlang politiek te gevoelig, maar inmiddels is er munitie voor de MQ-9-drones aangeschaft (zie hoofdstuk 15). Dit illustreert dat grenzen kunnen opschuiven. Dit geldt mogelijk ook voor het gebruik van technologie voor de tanden van de politie.[26]

Het hart van de politie

In de documentaire 'Tygo in de GHB' gaat een van de verhaallijnen over Junita.[27] Junita woont in het Brabantse Sint-Willebrord, is 28 jaar en al jaren zwaar verslaafd aan de drug GHB. Ze wil graag kinderen en een 'gewoon' leven, maar het lukt haar niet om van de GHB af te komen. Ze is blij dat Fred van Opstal – de wijkagent – regelmatig bij haar langskomt. Ze heeft iemand nodig die 'autoritair' is en haar 'in bedwang houdt'. In de documentaire valt op dat Fred weinig invloed heeft op het GHB gebruik van Janita, maar niettemin blijft langskomen en haar ondersteunt in haar leven.

De wijkagent geeft invulling aan wat ik het hart van de politie noem.[28] Dit is het relationele vermogen van de politie waarin betekenisvolle ontmoetingen tussen politiemensen en burgers centraal staan.[29] Het draait om *presentie*:[30] de politiemens die zich aandachtig en toegewijd op de ander betrekt en zo leert zien wat er bij de ander op het spel staat en gedaan zou kunnen worden en wie hij (de politiemens) hierbij voor de ander kan zijn.[31] Het relationele vermogen heeft geen ander doel dan relatievorming.[32] Hiervoor is compassionele rechtvaardigheid essentieel: '… het vermogen en de bereidheid burgers in een grote verscheidenheid van situaties tot hun recht te laten komen. Niet slechts door het tonen van begrip en medeleven, maar ook door actief voor hen op te komen.'[33]

Wat is de invloed van het gebruik van opkomende technologieën op het relationele vermogen van de politie? Die invloed is nihil. De politie zal in interactie met burgers weliswaar in toenemende mate gebruikmaken van softwarerobots – vaak in de vorm

26 Zie ook De Kool, Vermeeren & Steijn (2023) over dat in de toekomst de inzet van een 'killer robot' door de politie in de VS niet kan worden uitgesloten.

27 Het betreft een documentaire die in 2018 bij de NPO is uitgezonden. Zie ook https://www.bd.nl/den-bosch-vught/brabant-staat-centraal-in-docu-tygo-in-de-ghb-het-is-hier-zo-n-groot-probleem (voor het laatst geraadpleegd op 27 december 2019).

28 Zie voor meer verhalen o.a. Haest 2011.

29 Zie ook Van Hoorn 2011.

30 Andries Baart publiceerde in 2001 zijn theorie over presentie. Sindsdien is presentie uitgegroeid tot een begrip in de wereld van de professionele zorg- en hulpverlening. Naar mijn mening is de presentatietheorie een belangrijke theoretische grondslag voor het relationele vermogen van de politie.

31 Zie Beurskens, Van der Linde & Baart 2019.

32 Deze manier van denken vanuit de presentietheorie komt overeen met het werk van Jan Nap (2012) die stelt dat de kern van het politiewerk meer draait om de ontmoeting tussen burgers en politiemensen dan om de uitkomst van die ontmoeting.

33 Denkers 2001: 107.

van chatbots – maar een softwarerobot zal Fred Opstal en zijn verbinding met Janita niet kunnen vervangen. Sherry Turkle – hoogleraar aan het Massachusetts Institute of Technology – onderzoekt al geruime tijd de impact van AI op mensen. In haar memoires *The empathy diaries* betoogt ze dat AI-systemen kunnen leren om te denken en te praten, maar niet om empathisch te zijn.[34] De kracht van empathie onderscheidt mensen van de slimme systemen die hen proberen dicht te benaderen en op onderdelen ook kunnen overtreffen. Dit gegeven bepaalt volgens haar dat wij in het tijdperk van AI onze menselijkheid zullen behouden.[35] En dit geldt ook voor politiemensen. Voor het relationele vermogen van de politie zijn politiemensen nodig. Vandaag, morgen en overmorgen.

Betekenisgevers zonder hersens en lichaam

Het voorgaande maakt duidelijk dat het gebruik van technologie ertoe leidt dat een deel van de vermogens die de politie inzet voor haar taakuitvoering worden 'ontkoppeld' van politiemensen.[36] Er zijn in mindere mate politiemensen nodig om deze vermogens te realiseren. Een deel van de menselijkheid verdwijnt hiermee uit de politieorganisatie.[37] Dit is een fundamentele ontwikkeling: in het politiewerk aan de horizon ontstaan in toenemende mate betekenisgevers zonder hersens en zonder lichaam. Het politiewerk wordt in toenemende mate 'faceless'.[38] Om het concreet te maken: een MONOcam kan een burger niet stilhouden en met een burger een gesprek voeren over het leed dat het gebruik van een mobiele telefoon achter het stuur (bij anderen) kan veroorzaken. Dit geldt ook binnen de politieorganisatie: politiemensen werken samen met softwarerobots waarmee zij in beperkte mate kunnen communiceren. De ontwikkeling naar betekenisgevers zonder hersens en lichaam impliceert tevens dat de betekenisgeving minder persoonlijk of contextueel van aard wordt.[39] Burgers worden in toenemende mate 'bekeken' als een verzameling van datapunten in plaats van 'gezien' als mens. De optelsom hiervan is dat de verandering in de wijze waarop bepaalde politievermogens (ogen, brein) worden uitgeoefend, bijdraagt aan het *abstracter worden* van de politie.[40] Relaties binnen de politieorganisatie en tussen de politie en 'de' burger krijgen een meer onpersoonlijk karakter. Een relevante vraag is of we zo'n politie in onze samenleving willen hebben.

34 Turkle 2021.

35 Idealiter bieden opkomende technologieën de mogelijkheid om meer te investeren in het relationele vermogen van de politie, omdat er minder tijd aan informatieverwerking en administratieve taken hoeft te worden besteed. De tijd die 'overblijft', kan worden ingezet voor de taken die door politiemensen moeten worden uitgevoerd (zie ook Interpol & UNICRI, 2019). In de literatuur over AI wordt dit ook wel *rehumanizing time* genoemd (Daugherty & Wilson, 2018).

36 Zie in breder verband Harari (2017) over de 'grote ontkoppeling' waarmee hij verwijst naar de 'ontkoppeling' van bewustzijn en intelligentie die plaatsvindt als gevolg van AI.

37 Zie in meer algemene zin: Februari 2023.

38 Marciniak 2021.

39 Idem.

40 Zie Terpstra, Fyfe & Salet 2019.

22 Politiemodel

De technologiepraktijken die in deel III van dit boek zijn behandeld, worden in zowel de politiewetenschap als de -praktijk regelmatig aangeduid met relatief nieuwe termen. In de internationale context gaat het dan om *big data policing* en *data-driven policing*.[1] In de nationale context is het gebruik van *datagedreven werken* in zwang geraakt. Deze termen doen vermoeden dat er sprake is van een nieuw politiemodel of een nieuwe politiestrategie. In dit hoofdstuk ga ik in op de vraag of er (naar mijn idee) aanleiding is om van een nieuw politiemodel te (kunnen) spreken en zo ja, wat de wezenlijk nieuwe elementen van dit model zijn.

Datagedreven politiewerk in literatuur en praktijk

Big data policing en data-driven policing zijn – zoals gezegd – relatief nieuwe begrippen in de internationale politiewetenschap.[2] Over deze begrippen bestaat vooralsnog weinig conceptuele helderheid.[3] De rode draad is dat het gaat om politiewerk dat is gebaseerd op complexe analyses van grote hoeveelheden data uit verschillende bronnen.[4] In een rapport van de denktank voor de politie in het VK – *The Police Foundation* – wordt data-driven policing als volgt gedefinieerd:

> *'By data-driven, we mean the acquisition, analysis and use of a wide variety of digitized data sources to inform decision making, improve processes, and increase actionable intelligence for all personnel within a police service, whether they be operating at the front-line or in positions of strategic leadership.'*[5]

De politiewetenschap helpt vooralsnog weinig bij het definiëren van datagedreven politiewerk. Daarom gaan we te rade bij de praktijk. Binnen de politie in Nederland is de basis voor dit nieuwe concept gelegd door het THTC van de landelijke eenheid.[6] Deze ontstaansplek is niet toevallig, want dit team houdt zich bezig met de aanpak van *high tech* cybercriminaliteit en werkt in dit kader vrijwel uitsluitend met grote hoeveelheden digitale data.[7] Kenmerkend is dat deze data niet zijn gegenereerd door handelin-

1 De term *algorithmic policing* wordt ook met enige regelmaat gebruikt. Hiermee wordt verwezen naar de inzet van algoritmen in het politiewerk en (breder) de politiefunctie. Zie bijvoorbeeld Wessels 2023.
2 Zie bijvoorbeeld Ferguson 2017a; Kearns & Muir 2019; Marciniak 2021; Terpstra & Salet 2020.
3 Schuilenburg 2023.
4 Terpstra & Salet 2020.
5 Kearns & Muir 2019: 6.
6 Zie ook Hirsch Ballin & Oerlemans 2023.
7 Van de Sandt et al. 2022; Van den Eeden et al. 2021.

gen van de politie, maar al in de samenleving beschikbaar zijn en door de politie worden aangetroffen. Het betreft zogenaamde *found data*.[8] Ten behoeve van een effectieve en efficiëntie manier van omgaan met data heeft men vanaf 2016 een nieuwe, datagedreven manier van werken ontwikkeld.[9] Dit heeft geleid tot een operationeel model voor datagedreven bestrijden.
De kern van het model is een cyclisch proces dat bestaat uit vier fasen: verzamelen, opslaan, analyseren en interveniëren (zie hoofdstuk 18).[10] In de fase van verzamelen worden databronnen geïdentificeerd en geprioriteerd waarbij diversiteit in bronnen wordt nagestreefd. Per bron wordt nagegaan wat er nodig is om de bron te ontsluiten en wat de risico's zijn. Daarna worden data verzameld. De data uit de verschillende bronnen worden vervolgens in een gemeenschappelijke datastructuur bij elkaar gebracht en opgeslagen. De derde fase is analyse op basis van datawetenschappelijke methoden en technieken, in combinatie met domeinkennis van onder andere analisten. Data worden gecombineerd en verrijkt met reeds bekende informatie. Op basis van het beeld dat hierdoor ontstaat, wordt zo objectief mogelijk bepaald wat vermoedelijk de meest effectieve en efficiënte interventies zijn. Deze interventies leveren weer nieuwe data op waarmee de cyclus van datagedreven bestrijden opnieuw wordt doorlopen. Deze manier van werken wordt binnen door de politie beschouwd als een nieuw paradigma waarin traditionele (tactische) expertise, de meer recente digitale expertise en de nieuwe datawetenschappelijke expertise met elkaar worden gecombineerd.[11]

Het concept van datagedreven bestrijden is weliswaar ontstaan in het kader van de aanpak van cybercriminaliteit, maar is na verloop van tijd breder toegepast binnen de opsporing. Bij de opsporing op basis van cryptocommunicatiedata is men binnen de politie de term 'datagedreven opsporen' gaan gebruiken (zie hoofdstuk 12). Datagedreven opsporen wordt gekenmerkt door een op onderdelen ander werkproces dan voorheen: van zaak zoekt bewijs naar bewijs zoekt zaak. In de bulkdata die in één operatie verkregen zijn, bevindt zich bewijs voor allerlei andere gepleegde strafbare feiten. Door de data – onder voorwaarden – te doorzoeken, kunnen relevante data worden geselecteerd en voor opsporingsonderzoek worden gebruikt. Op deze wijze ontdekt de politie strafbare feiten in de data.[12] De informatiepositie bij de start van een opsporingsonderzoek verschilt daarmee fundamenteel van de 'traditionele' situatie waarin signalen – bijvoorbeeld vanuit Meld Misdaad Anoniem of criminele inlichtingen – worden opgewerkt tot een informatiepositie die voldoende is om een projectmatig onderzoek te

8 Kitchin, 2014; zie ook Brayne 2021.
9 Van de Sandt et al. 2022.
10 In publicaties van de grondlegger(s) worden veelal Engelse termen gebruikt – collect, store, analyse, engage – die worden samengevat als het CSAE-raamwerk (zie onder andere Van de Sandt et al. 2022; zie ook hoofdstuk 18). Hierbij moet worden benadrukt dat dit raamwerk bestaat uit verschillende elementen, waaronder het bedrijfsproces, dataschema en publieke waardenfilosofie. In deze paragraaf focus ik vooral op het bedrijfsproces en doe ik geen recht aan het gehele raamwerk.
11 Van de Sandt et al. 2022.
12 Hirsch Ballin & Oerlemans 2023.

kunnen starten.[13] Als gevolg van de cryptocommunicatiedata is het bereik van deze manier van werken flink uitgebreid.

> *'… het concept van datagedreven opsporing en de cryptotelefoonoperaties zijn geen "high tech"-operaties in de marge van de opsporing, maar spelen een wezenlijke rol in de strafrechtspleging en leiden tot een fundamentele verschuiving in de werkwijze van de opsporing.'*[14]

Van 'datagedreven opsporen' is vervolgens de stap gezet naar 'datagedreven werken'. Deze stap is onder andere zichtbaar in het (door de minister van J&V overgenomen) advies van de Adviescommissie voor de Landelijke Eenheid dat in 2022 is uitgebracht:

> *'Naar het oordeel van de commissie vraagt een toekomstbestendige aanpak van veiligheidsdreigingen om datagedreven werken… De commissie beveelt aan om deze datagedreven manier van werken – die veel verder strekt dan enkel de inzet van moderne technologie maar wel gebaseerd is op technologie – snel en breed uit te rollen binnen de beide nieuw te vormen landelijke eenheden en deze werkwijze dus niet alleen voor een deel van de opsporing toe te passen... De intensivering van datagedreven werken binnen de twee landelijke eenheden zou zo de aanjager kunnen zijn voor een transitie binnen het hele korps.'*[15]

Dit citaat maakt duidelijk dat datagedreven werken als een relevante manier van werken voor het gehele politiewerk wordt gezien: datagedreven politiewerk.[16] Daarnaast wordt gewezen op een belangrijk kenmerk dat in de praktijk aan datagedreven politiewerk wordt toegeschreven: het gebruik van moderne (datagedreven) technologie in het politiewerk.[17]

Bovenstaande uiteenzetting maakt duidelijk dat het begrip 'datagedreven politiewerk' in de praktijk een nadere invulling heeft gekregen. Deze invulling is echter niet eendui-

---

13 De cryptocommunicatiedata gaan over georganiseerde (haal)criminaliteit, wat wil zeggen dat de werkwijze van 'bewijs zoekt zaak' in dit verband veelal geen betrekking heeft op aangiftecriminaliteit (ook wel brengcriminaliteit genoemd).

14 Hirsch Ballin & Oerlemans 2023: 24.

15 Adviescommissie Landelijke Eenheid 2022: 34-36.

16 De voorbeelden uit deel III van dit boek maken wat mij betreft duidelijk dat er al meer praktijken zijn waarin het cyclische proces van verzamelen, opslaan, analyseren en interveniëren te herkennen is. Hierbij kan onder andere worden gedacht aan het gebruik van geavanceerde platformen en analysesoftware – zoals de Raffinaderij – ten behoeve van opsporingsonderzoek (breder dan cryptocommunicatiedata), realtime intelligence, veiligheidsanalyse en predictive policing. Deze praktijken doen zich voor in het intelligencewerk, het rechercheerwerk en het politiestraatwerk. De gewenste, datagedreven manier van werken – ik noem het datagedreven politiewerk – komt dus al tot ontwikkeling in andere disciplines dan de opsporing en in andere eenheden dan de landelijk eenheid. Hierbij moet wel worden opgemerkt dat het op een meer gedetailleerd niveau verschillende manieren van werken betreft. De rode draad is het proces van verzamelen, opslaan, analyseren en interveniëren met gebruik van datawetenschappelijke methoden.

17 Zie ook Snaphaan et al. (2023) die stellen dat een brede of ruime opvatting van big data policing ook oog heeft voor de verwerking, analyse en het gebruik van data (met behulp van moderne technologie).

dig. Er zijn – naar mijn idee – drie betekenissen van 'datagedreven' in relatie tot politiewerk te identificeren. Hoewel deze betekenissen (deels) overlappen en samenhangen, is het naar mijn idee zinvol om ze te onderscheiden. Het zijn:

1. Datagedreven in de betekenis van het verzamelen, opslaan en analyseren van data ten behoeve van intelligence die wordt gebruikt om het politieoptreden te sturen. De ontwikkelingen op het gebied van veiligheidsanalyse vallen hieronder, maar ook realtime intelligence en predictive policing kunnen op deze wijze worden beschouwd.
2. Datagedreven in de betekenis van 'bewijs zoekt zaak', wat wil zeggen dat de politie in (bulk)data op zoek gaat naar strafbare feiten en de hierbij betrokken verdachten én het bewijs (hoofdzakelijk) uit deze data haalt.[18] De casuïstiek op het gebied van cryptocommunicatiedata is hiervan hét voorbeeld, maar deze manier van werken wordt ook voor andere databronnen gebruikt (zie ook hoofdstuk 13, 18 en 27).
3. Datagedreven in de betekenis van het gebruik van datagedreven technologie (AI) ten behoeve van het verbeteren van de sturing en uitvoering van politiewerk. In deel III van dit boek zijn vele voorbeelden van dit gebruik gegeven. Er wordt binnen de politie in Nederland aan de ontwikkeling van AI gewerkt ter ondersteuning van een groot aantal werkprocessen.[19] Het gaat dan niet alleen om de primaire processen, maar ook om allerlei secundaire processen.

Datagedreven politiewerk als nieuw politiemodel?

In de politiewetenschap wordt er geregeld gepubliceerd over de wijze waarop de politie in Nederland invulling geeft aan onder andere gebiedsgebonden politiewerk (*community policing*) en informatiegestuurd politiewerk (*intelligence-led policing*). Gebiedsgebonden politiewerk (GGP) of informatiegestuurd politiewerk (IGP) wordt dan vaak aangeduid als een 'concept', 'politiemodel' of 'politiestrategie'. Vervolgens wordt GGP of IGP gedefinieerd, maar wordt niet ingegaan op de overkoepelende term 'concept', 'model' of 'strategie'. In het kader van de centrale vraag in dit hoofdstuk is dit echter wel van belang. Ik hanteer de term politiemodel en beschouw een model als een (min of meer) samenhangend geheel van uitgangspunten ten aanzien van de organisatie, sturing en uitvoering van politiewerk. De veronderstelling die veelal in een politiemodel besloten ligt, is dat het in de praktijk realiseren van de uitgangspunten leidt tot effectief politiewerk (zie hoofdstuk 26 over het problematische karakter van het effectiviteitsbegrip).

Er zijn in de afgelopen decennia in de internationale politiewetenschap verschillende politiemodellen gedefinieerd.[20] De voornaamste modellen zijn het eerdergenoemde *community policing* en *intelligence-led policing* en in mindere mate *problem-oriented*

18 Hirsch Ballin & Oerlemans (2023) definiëren datagedreven opsporing in dit verband als de verwerking van gegevens die eerder door de politie bij hun taakuitoefening in andere onderzoeken zijn verzameld en daarna ten behoeve van nieuwe opsporingsonderzoeken worden geanalyseerd.

19 Testerink, Nieuwenhuizen & Bex 2023.

20 Zie voor een overzicht onder andere de tweede editie van de bundel van Weisburd & Braga (2019) over *police innovation*.

policing (POP) en *evidence-based policing* (EBP). Een uitwerking en vergelijking van deze modellen valt buiten het doel van dit boek.[21] Ik beperk me tot enkele algemene constateringen. De eerste constatering is dat de mate waarin een politiemodel van toepassing is op alle politietaken verschilt. Er ligt in algemene zin veel nadruk op het politiestraatwerk dat door geüniformeerde politiemensen wordt uitgevoerd.[22] De tweede constatering is dat de mate waarin een model is uitgewerkt in termen van organisatie, sturing en uitvoering van politiewerk tussen de modellen uiteenloopt. Ik beschouw GGP en IGP als de meest uitgewerkte modellen, wat onder andere wil zeggen dat op verschillende elementen (organisatie, sturing, uitvoering) en concreet kan worden aangegeven wat de consequenties van implementatie van het betreffende model zijn. De derde constatering is dat de modellen in conceptuele zin verschillen, maar ook overeenkomsten vertonen.[23] Zo wordt er bij zowel problem-oriented policing als intelligence-led policing vanuit gegaan dat analyse de basis moet zijn voor de wijze waarop de politie (samen met partners) veiligheidsproblemen aanpakt. De vierde – hiermee samenhangende – constatering is dat de politiemodellen in de praktijk naast elkaar bestaan.[24] De vijfde constatering is dat de mate waarin een politiemodel in de praktijk tot wasdom komt in de tijd kan verschillen. Zo wordt op dit moment in Nederland het GGP model minder in de praktijk gebracht dan toen ik – bijna twintig jaar geleden – begon met politieonderzoek.[25] Het IGP model is in dezelfde periode dominanter geworden, wat onder andere zichtbaar is in het ontstaan van een aparte intelligenceorganisatie.[26]

Dan nu naar de vraag of datagedreven politiewerk een nieuw politiemodel is. Het beantwoorden van deze vraag wordt bemoeilijkt door de verschillende betekenissen die datagedreven politiewerk heeft. Om die reden behandel ik achtereenvolgens de verschillende betekenissen.
De eerste betekenis van datagedreven politiewerk komt in behoorlijke mate overeen met een al bestaand politiemodel, te weten: IGP.[27] IGP wil zeggen dat beslissingen over de aanpak van veiligheidsproblemen en uitvoering van de politietaak worden genomen op basis van geanalyseerde informatie en kennis.[28] Jerry Ratcliffe definieert dit politiemodel als volgt:

21 Zie hiervoor onder andere: Van Steden, Anholt & Koetsier 2021.
22 Brodeur 2010.
23 Zie ook Van Steden, Anholt & Koetsier 2021.
24 Zie ook Niculescu-Dincă 2016.
25 Zie ook Terpstra 2019.
26 Zie ook Landman, Kouwenhoven & Brussen 2020.
27 Hierbij moet worden opgemerkt dat ILP op diens beurt weer enige conceptuele overlap heeft met onder andere problem-oriented policing en community policing. Dit was voor het voormalig regiokorps Haaglanden aanleiding om te investeren in 'the best of three worlds': een combinatie van de politiemodellen (zie Versteegh, van der Plas & Nieuwstraten, 2011).
28 Kop & Klerks 2009; Ten Brink, Ter Mors & Den Hengst 2017.

> *'Intelligence-led policing emphasizes analysis and intelligence as pivotal to an objective, decision-making framework that priorities crime hot spots, repeat victims, prolific offenders and criminal groups. It facilitates crime and harm reduction, disruption and prevention through strategic and tactical management, deployment, and enforcement.'*[29]

De definitie van IGP lijkt op onderdelen op de eerder behandelde definitie van datagedreven politiewerk. Daarnaast vertoont het intelligenceproces veel overeenkomsten met het proces van datagedreven politiewerk: verzamelen, opslaan, analyseren en interveniëren.[30] In beide modellen heeft analyse een belangrijke plek, omdat analyse moet leiden tot een min of meer objectieve basis voor besluitvorming over de inzet van uiteenlopende interventies. Beide modellen kunnen daarmee ook de basis zijn voor andere politiemodellen en dan in het bijzonder voor probleemgericht politiewerk waarbij op basis van analyse operationele strategieën worden ontwikkeld en wordt getracht inzicht te krijgen in de effecten van deze operationele strategieën.[31] De overlap tussen datagedreven politiewerk en intelligencegestuurd politiewerk is ook zichtbaar in de literatuur: verschillende praktijken uit dit boek worden in uiteenlopende publicaties onder de noemer van intelligencegestuurd politiewerk geschaard. Het gaat dan onder andere om realtime intelligence, veiligheidsanalyse en ook predictive policing.[32] Ook binnen de politie wordt door betrokkenen geregeld aangegeven dat datagedreven politiewerk min of meer een synoniem is voor IGP.[33] Het wordt in het verlengde hiervan gezien als een impuls om een volgende stap in de uitwerking en ontwikkeling van IGP te zetten. In essentie is dan er dan dus niets nieuws onder de zon. Kortom: de eerste betekenis van datagedreven politiewerk levert geen nieuw politiemodel op.

De tweede betekenis van 'datagedreven' verwijst naar een manier waarop politiewerk wordt uitgevoerd. Het gaat dan in het bijzonder om opsporing. Deze manier van uitvoeren is naar mijn idee nieuw: in *onderdelen* van de opsporing is er sprake van een (wezenlijk) andere manier van werken dan voorheen. In deze manier van werken staat het verwerken van grote hoeveelheden data met gebruik van technologie – zoals de Raffinaderij – centraal (zie ook hoofdstuk 13).[34] Het gaat dan niet alleen of zozeer om sturing – zoals bij IGP – maar (ook) om de uitvoering van het politiewerk. Rechercheurs verrichten ander werk dan dat zij deden: minder zelf opsporingsmethoden inzetten en meer bestaande data analyseren. Het nieuwe karakter van de manier van werken is ook merkbaar aan wat het oproept bij in het bijzonder de strafrechtadvoca-

29 Ratcliffe 2016: 66.
30 Zie bijvoorbeeld de uitwerking van Duijn 2011.
31 De brede bestrijdingsstrategie van het THTC kun je naar mijn idee ook zien als een toepassing van probleemgericht politiewerk. Zie hoofdstuk 18.
32 Zie ook Ten Brink, Ter Mos & Den Hengst 2017.
33 Den Hengst & Wijsman 2023. Zie ook het voorwoord van de landelijk portefeuillehouder Intelligence – Jannine van den Berg – in de derde editie van het magazine *Scherp over intelligencegestuurd politiewerk* (juli 2023).
34 Zie ook Fedorova et al. 2022.

tuur. Zij hebben te maken met nieuwe omstandigheden en spreken zich hierover uit. Een nieuwe manier van werken in (een deel van) de opsporing wil tegelijkertijd nog niet zeggen dat er in de praktijk sprake is van een nieuw politiemodel. Wil er sprake zijn van een nieuw politiemodel, dan is een bredere toepassing (naar mijn idee) nodig. Dit roept de vraag op of de essentie van de manier van werken in de opsporing ook toepasbaar is bij het uitvoeren van andere hoofdtaken van de politie. Een dergelijke, bredere toepassing wil zeggen dat data een steeds grotere rol spelen in de wijze waarop de politie haar 'waarde' in de samenleving levert. In het politiewerk zal er dan meer focus komen te liggen op het verzamelen, registreren, bewerken, opslaan en analyseren van data.[35] Indien deze ontwikkeling daadwerkelijk gaat plaatsvinden, kan er – mijn inziens – worden gesproken van een nieuw politiemodel. Het is echter de vraag of dit een realistisch perspectief is. Het kan immers ook zo zijn dat er vooral wezenlijke veranderingen in (onderdelen van) de opsporing plaatsvinden.

De derde betekenis van 'datagedreven' heeft betrekking op het gebruik van datagedreven technologie in de sturing en uitvoering van het politiewerk.[36] Datagedreven politiewerk wil dan simpel gesteld zeggen: politiewerk met gebruik van algoritmen of meer specifiek: met gebruik van AI. Deze betekenis heeft een relatie met de eerste en tweede betekenis, omdat datagestuurde technologieën (ook) worden ingezet voor zowel de doorontwikkeling van IGP (sturingsconcept) als de uitvoering van uiteenlopend politiewerk (opsporing, maar ook dienstverlening, noodhulp, handhaving).[37] De opkomst van het gebruik van datagedreven technologie in het politiewerk in het algemeen en AI in het bijzonder is naar mijn idee een fundamentele ontwikkeling.[38] Het fundamentele karakter van deze ontwikkeling vloeit voort uit de veranderende rol van technologie in het politiewerk (zie hoofdstuk 20): van ondersteunend naar vormend en soms disciplinerend, van secundair naar primair, van de randen naar de kern.[39] Dit uit zich onder andere in het versterken en overnemen van processen van betekenisgeving van

35 In 1997 publiceerden Richard Ericson en Kevin Haggerty hun boek *Policing the risk society* dat in zekere zin – en met terugwerkende kracht – kan worden beschouwd als de vooraankondiging van deze ontwikkeling (zie ook Shon & O'Connor, 2020). Op basis van empirisch onderzoek in Canada betoogden zij dat politiemensen in toenemende mate kenniswerkers zijn die zich bezighouden met het verzamelen van informatie ten behoeve van andere instituties die gericht zijn op allerlei vormen van risicobeheersing. Het boek was zijn tijd vermoedelijk ver vooruit, maar elementen van hun theorie over nieuw politiewerk komen op dit moment in toenemende mate in de praktijk tot uiting.

36 Zie ook Van de Sandt et al. (2022) die erop wijzen dat datawetenschappelijke methoden en technieken hun weg naar het politiewerk hebben gevonden. Zij constateren dat dit een nieuwe ontwikkeling is.

37 Dit maakt ook duidelijk dat de drie betekenissen niet 'strak' van elkaar zijn te onderscheiden. Naar mijn idee geldt dit vooral voor de derde betekenis ten opzichte van de eerste en tweede betekenis. Het is naar mijn mening van meerwaarde om de eerste en tweede betekenis van elkaar te onderscheiden, omdat intelligence iets anders is dan bewijs (zie ook Duijn, 2011). In sommige publicaties over datagedreven werken worden intelligence en bewijs mijns inziens te veel door elkaar gehaald.

38 Zie ook Joh 2018b.

39 Zie ook Niculescu-Dincă 2016.

politiemensen met een substantiële uitbreiding van het vermogen tot waarnemen (data verzamelen) en data verwerken tot gevolg.[1]

> *'Artificial intelligence has begun to change the capabilities of the police by permitting them to do what was once nearly impossible or impracticable.'*[2]

AI leidt op onderdelen tot een verandering in de wijze waarop politiewerk wordt uitgevoerd.[3] De uitbreiding van het vermogen tot het verzamelen en analyseren van data heeft daarnaast als gevolg dat er een nieuw, datagedreven, type kennis in de politieorganisatie ontstaat. Deze kennis heeft een ander karakter dan de professionele intuïtie die vooralsnog dominant is in veel vormen van politiewerk.[4] De nieuwe, datagedreven inzichten gaan naar verwachting steeds meer interacteren met de kennis van politiemensen. Dit wil zeggen dat datagedreven werken (ook) wordt gekenmerkt door samenwerking tussen politiemens en politiemachine (zie hoofdstuk 25). De vraag is of de veranderende relatie tussen politiewerk en technologie het rechtvaardigt om een nieuw politiemodel te introduceren. In het antwoord op deze vraag zijn twee redenaties mogelijk. De ene redenatie is dat technologiegebruik kan worden beschouwd als onderdeel van andere politiemodellen.[5] Het heeft vanuit dit perspectief weinig meerwaarde om een nieuw politiemodel te introduceren. De andere redenatie is dat de veranderingen die nu gaande en aanstaande zijn een fundamenteel karakter hebben én niet of nauwelijks worden meegenomen in de bestaande politiemodellen. Deze redenatie leidt tot de uitkomst dat er reden is om een nieuw politiemodel te introduceren, te weten: datagedreven politiewerk.

Op basis van het voorgaande ben ik geneigd om het antwoord op de vraag of er sprake is van een nieuw politiemodel met een voorzichtige 'ja' te beantwoorden. Dit wil vooral zeggen dat datagedreven politiewerk de potentie heeft om een nieuw politiemodel te worden. Dit model wordt vooral gekenmerkt door 1) een breed *in de politieoperatie* ingebed proces van verzamelen, opslaan en analyseren van data als basis voor het optreden, en 2) het gebruik van (zelflerende) algoritmen voor de uitvoering van het politiewerk in het algemeen en het proces van verzamelen, opslaan en analyseren van data in het bijzonder. Om dit politiemodel (verder) in de praktijk te brengen, staat de politieorganisatie voor uiteenlopende uitdagingen. Dit is het thema van het volgende hoofdstuk.

1 Het is van belang te benadrukken dat ik me hier beperk tot de uitvoering van politiewerk. AI heeft binnen de politieorganisatie een breder toepassingsgebied en dit is ook zichtbaar in de ontwikkelingen die gaande zijn.
2 Joh 2018b: 284-285.
3 Zie ook Wessels 2023.
4 Ratcliffe, Taylor & Fisher 2020; zie ook Landman 2015.
5 Zie bijvoorbeeld Niculescu-Dincă 2016 voor een dergelijke uitwerking.

23 Politieorganisatie

De opkomst van nieuwe technologieën vraagt – via zowel het veranderende veiligheidsvraagstuk als de toepassing van technologie in het politiewerk – om veranderingen in de politieorganisatie. Deze veranderingen worden tezamen ook wel de digitale transformatie genoemd.[6] In dit hoofdstuk staan deze veranderingen centraal. De nadruk ligt hierbij meer op de veranderingen die samenhangen met de toepassing van technologie in het politiewerk dan op de veranderingen die samenhangen met het veranderende veiligheidsvraagstuk.[7] Het gaat dan in het bijzonder om datagedreven politiewerk dat wordt gekenmerkt door een breed in de politieoperatie ingebed proces van verzamelen, opslaan en analyseren van data als basis voor het politiewerk waarbij gebruik wordt gemaakt van AI (zie hoofdstuk 22). Ik beschrijf in dit hoofdstuk een deel van de veranderingen die van de politieorganisatie worden gevraagd en geef waar mogelijk aan hoe deze op dit moment invulling krijgen.[8] Hierbij maak ik onderscheid tussen strategie, informatievoorziening, personeel, organisatiemodel en cultuur.

Strategie: weten wat je ermee wilt bereiken

Binnen de politieorganisatie zijn er vele toepassingen mogelijk van digitale technologie in het algemeen en AI in het bijzonder.[9] Dit heeft verschillende oorzaken. Een van de voornaamste oorzaken is dat de sturing en uitvoering van politiewerk voor een (soms groot) deel bestaan uit gegevensverzameling en -verwerking. Anders gezegd: politiewerk is tot op zekere hoogte informatiewerk. Informatiewerk heeft baat bij de digitale technologieën die nu opkomen. Het gebruik ervan kan waarde toevoegen aan de sturing en uitvoering van politiewerk (zie ook hoofdstuk 26). Onderzoekers van de universiteiten van Leiden en Delft stellen:

> *'Having in mind the possible benefits that AI can provide in the law enforcement domain, the police cannot ignore this technology. The question is not if AI should be used, by what it is most suited for and how it can properly implemented.'*[10]

6 Zie ook de algemene organisatieliteratuur, bijvoorbeeld: Hanelt et al. 2021; Kraus et al. 2021.
7 Deze kunnen – zoals in hoofdstuk 1 is aangegeven – samenhangen, maar dat hoeft niet.
8 De gevolgen voor het politievakmanschap behandel ik in hoofdstuk 25. Deze gevolgen horen ook bij de digitale transformatie. Daarnaast wil ik nogmaals benadrukken dat (in het bijzonder) dit hoofdstuk verre van compleet is. Het betreft een selectie van onderwerpen en invalshoeken.
9 Zie ook Dechesne et al. 2019.
10 Dechesne et al. 2019: 5.

In het verlengde van bovenstaand citaat wordt in de literatuur over het gebruik van AI in organisaties aangegeven dat de gevolgen voor de strategie van de organisatie tweeledig (moeten) zijn. Het gebruik van AI dient in de eerste plaats onderdeel te worden van de organisatiebrede strategie. Hierbij moet 'de' organisatie scherp voor ogen hebben hoe AI bijdraagt aan de organisatiebrede strategie en -doelstellingen. Thomas Davenport en Nitin Mittal van het adviesbureau Deloitte maken in hun boek *All in on AI* een onderscheid tussen drie archetypen voor deze bijdrage: 1) iets nieuws creëren (een nieuw bedrijfsmodel), 2) transformeren van de operatie, of 3) beïnvloeden van het gedrag van klanten.[11] De tweede implicatie op het niveau van strategie is dat er een strategie op het gebied van AI nodig is. De kern van deze strategie moet bestaan uit een overzicht en prioritering van *use cases*.[12] Een use case beschrijft wat een bepaalde toepassing van AI bijdraagt aan de doelstellingen van de organisatie. Het uitgangspunt hierbij is dat er wordt gekozen voor use cases die de bredere organisatiestrategie ondersteunen. Wat zijn de use cases met veel (gewenste) impact?[13] Scherpte is (ook) hierbij van belang: AI moet bepaalde problemen oplossen of kansen benutten.[14] Dat is niet abstract, maar concreet. Het risico van te algemene noties is dat er vooral wordt geïnvesteerd in AI om zodoende 'de boot niet te missen'.[15] Dat is een zwak fundament. De AI-strategie moet daarnaast richting geven aan de organisatieontwikkeling die nodig is om (zo optimaal mogelijk) datagedreven te kunnen werken.[16] Het gaat dan onder andere om de informatievoorziening, vaardigheden van personeel en cultuur. De AI-strategie moet onder regie van de eindverantwoordelijke bestuurder worden uitgevoerd.[17]

Het voorgaande heeft als consequentie dat (onder andere) leidinggevenden op bestuurlijk-strategisch niveau een goed begrip van AI moet hebben.[18] Wat is het? Wat kun je ermee binnen de politieorganisatie? In welke use cases moet je als politieorganisatie investeren en in welke juist niet? Wat vraagt het ontwikkelen, implementeren en gebruiken van AI toepassingen van de politieorganisatie in termen van verandering van werkprocessen, ontwikkeling van personeel en dergelijke? Hoe kun je de meerwaarde van AI toepassingen in kaart brengen? Dit zijn voorbeelden van vragen waarop leidinggevenden op bestuurlijk-strategisch niveau een antwoord moeten kunnen geven. De eerder aangehaalde Davenport & Mittal benadrukken in het verlengde hiervan dat de keuze van use cases niet teveel bottom-up tot stand moet komen.[19] Leidinggevenden op bestuurlijk-strategisch niveau zijn nadrukkelijk aan zet. Zij hebben hierbij

11 Davenport & Mittal 2023.
12 Davenport & Mittal 2023; Ganesan 2022.
13 Agrawal, Gans & Goldfarb (2022) geven aan dat het hierbij helpt om de organisatie te beschouwen als een verzameling van beslissingen, omdat AI vooral besluitvorming (in allerlei verschijningsvormen) kan verbeteren. Voor welke beslissingen heeft de inzet van AI de meeste meerwaarde?
14 Ganesan 2022.
15 Maggiori 2023.
16 Borek & Prill 2020; Davenport & Mittal 2023.
17 Borek & Prill 2020; Thamm, Gramlich & Borek 2020.
18 Agrawal, Gans & Goldfarb 2022; Davenport & Mittal 2023; Ganesan 2022.
19 Davenport & Mittal 2023.

ondersteuning nodig. Dit wil onder andere zeggen dat er een organisatiefunctie moet zijn die ervoor zorgt dat technologische ontwikkelingen worden gemonitord en inschat welke toepassingen bijdragen aan de doelen van de organisatie.[20] Het is daarnaast van belang dat de leiding op verschillende niveaus gecommitteerd is om langdurig te investeren in AI.[21] Commitment uit zich onder andere in het beschikbaar stellen van budget[22] door de politietop en persoonlijke betrokkenheid bij cruciale projecten.

Op basis van literatuuronderzoek en lopende onderzoeksopdrachten binnen de politie heb ik de indruk dat de politie in Nederland bezig is met haar strategie op het gebied van AI. Hierbij beschouw ik strategie niet als een document, maar als een voortdurend proces. Ik baseer deze indruk op verschillende constateringen. Zo heeft de politie in Nederland een directie strategie & innovatie waar onder andere de genoemde monitorfunctie en expertise op het gebied van beleid (technologie, innovatie) zijn ingericht. Er is tevens een AI-strategie waarin wordt ingegaan op de use cases die als het meest waardevol worden beschouwd en tevens aandacht wordt besteed aan de organisatieontwikkeling die nodig is om AI binnen de politieorganisatie te benutten. Uit het vervolg van dit hoofdstuk zal blijken dat de politie in Nederland daadwerkelijk investeert in de benodigde organisatieontwikkeling, bijvoorbeeld voor wat betreft informatievoorziening en expertise op het gebied van datawetenschap. Wat – naar mijn indruk – nog ontbreekt, is scherpte in de bijdrage die AI aan de organisatiebrede strategie moet gaan leveren. Een tweede aandachtspunt is de sturing op de ontwikkeling en implementatie van use cases (zie ook 'organisatiemodel'). Er wordt (naar mijn idee) breed geïnvesteerd in use cases, terwijl meer focus wellicht wenselijk is. Bijvoorbeeld: is predictive mapping (het CAS, zie hoofdstuk 19) de investeringen wel waard? Een derde aandachtspunt is de AI-expertise van leidinggevenden op bestuurlijk-strategisch niveau. Deze expertise bevindt zich vooral om deze leidinggevenden heen. Ik sluit deze paragraaf om die reden af met een advies van Kavita Ganesan in *The businesscase AI*: 'One of the most valuable moves a company can make before attempting AI is to educate its executives on the topic.'[23]

Informatievoorziening: nieuwe platformen en harmonisatie

In organisaties die datagedreven werken wordt de informatievoorziening (IV) beschouwd als een strategisch bedrijfsmiddel dat centraal in de organisatie staat. Een tweede kenmerk is dat het onderscheid tussen IV en de 'business' vervaagt.[24] Informatievoorziening in het algemeen en AI in het bijzonder raken in toenemende mate ingebed in het operationele model van de organisatie.[25]

20 Idem.
21 Idem.
22 Aandacht voor het rendement van investeringen is van belang, maar het is tegelijkertijd niet wenselijk om hier te snel, teveel nadruk op te leggen, want dit kan het experimenteren met nieuwe toepassingen belemmeringen (er moet dan direct iets bruikbaars uitkomen).
23 Ganesan 2022: 152.
24 Zie in meer in algemene zin: Borek & Prill 2020.
25 Daugherty & Wilson 2022; Iansiti & Lakhani 2020.

> *'An AI-centric firm is not defined by the sophistication of any individual algorithm it deploys, but by the structure and processes that enable the quick deployment of many AI solutions, each solving a real business problem.'*[26]

Datagedreven werken vraagt om de aanwezigheid van verschillende componenten, *waaronder* datamanagement/data-infrastructuur[27], voorzieningen voor het ontwikkelen en testen van (zelflerende) algoritmen en de infrastructuur voor software.[28] Data zijn de brandstof en de algoritmen zijn de machines.[29] Het begint dus bij het vastleggen, opschonen, bewerken, opslaan en combineren van data.[30] Om datagedreven te kunnen werken, zijn er gecentraliseerde dataplatformen nodig.[31] Politieorganisaties wereldwijd hebben op dit gebied een opgave. Zij hebben – overigens net als veel private organisaties[32] – te maken met padafhankelijkheid: er zijn in het verleden allerlei keuzes gemaakt die gevolgen hebben voor hoe er op dit moment met data wordt omgegaan. Zo zijn data van oudsher opgeslagen in verschillende systemen.[33] Anders gezegd: er zijn silo's met eigen datastructuren en databases.[34] Dit heeft als gevolg dat data moeizaam kunnen worden gecombineerd. Dit is in de politieorganisatie in Nederland op dit moment een actueel knelpunt. 'Binnen het politiekorps wordt informatie nu vaak nog traditioneel verzameld, opgeslagen en geanalyseerd in separate systemen die zijn gerelateerd aan specifieke politietaken', zo concludeert de Adviescommissie voor de landelijke eenheid in 2022.[35] Dit geldt niet alleen voor de bedrijfsprocessensystemen waarin wordt geregistreerd, maar ook voor systemen die worden gebruikt voor het opslaan en ontsluiten van data. Een voorbeeld van een opslagsysteem is het digitaal transferium waar veiliggestelde data worden opgeslagen.[36] Een voorbeeld van een ontsluitingssysteem is iBase: er zijn verschillende iBase-omgevingen – per eenheid en/of per thema – waarin data uit verschillende registratiesystemen bij elkaar worden gebracht.

Politieorganisaties in uiteenlopende landen zijn bezig met het doorbreken van de silo's die het organiseren van data voor datagedreven politiewerk belemmeren. Dit geldt ook voor de politie in Nederland. Harmonisatie is hierbij het streven.[37] Dit betreft harmo-

26 Iansiti & Lakhani 2020: xxiv. Zie ook Davenport & Mittal 2023; Ganesan 2022.
27 Organisaties die de transformatie naar datagedreven werken hebben 'doorgemaakt', geven vaak aan dat het moderniseren van de data-infrastructuur een van de succesfactoren was (Davenport & Mittal, 2023). Het gaat dan om de wijze waarop data worden verzameld, opgeslagen, bewerkt en gebruikt waarbij een *single source of truth* een belangrijk principe is (zie ook DalleMule & Davenport, 2021).
28 Iansiti & Lakhani 2020; Ganesan 2022.
29 Zie ook Stolze 2018.
30 Zie ook Stephenson 2018.
31 Davenport & Mittal 2023; Iansiti & Lakhani 2020.
32 Borek & Prill 2020; Iansiti & Lakhani 2020; Rashedi 2022.
33 Dit worden ook wel *legacy systemen* genoemd: systemen die technisch zijn verouderd. Binnen de politie in Nederland zijn hier vele voorbeelden van, waaronder BVH. Een organisatie met veel legacy systemen heeft een meerjarenplan nodig om de technische randvoorwaarden voor datagedreven werken te kunnen realiseren (Davenport & Mittal, 2023).
34 Zie onder andere Brayne 2021; Egbert & Leese 2021; Manning 2008; Marciniak 2021; Sanders & Chan 2021; Van de Sandt et al. 2022.
35 Adviescommissie Landelijke Eenheid 2022: 33.
36 Zie ook Roest 2023.
37 Van de Sandt et al. 2022.

nisatie tussen politieonderdelen in Nederland, maar ook harmonisatie met partners in binnen- en buitenland. Ik richt me hier primair op de interne, technische harmonisatie.[38] Om data te kunnen gebruiken voor meerdere werkprocessen, is het van belang om data uniform op te slaan en samen te brengen op één plek.[39] In de internationale politieliteratuur wordt deze harmonisatie ook wel aangeduid met *platform policing.*[40]

> *'The most important trend, however, seems to be the move toward technical architectures that allow for the establishment of virtual, cloud-based analysis platforms that do away with the limitations of outdated databases and silo structures.'*[41]

Platformisatie heeft verschillende verschijningsvormen. Ik noem enkele ontwikkelingen die zich bij de politie in Nederland afspelen.[42] Het programma 'IV Next Base' is gericht op het verbeteren van de infrastructurele basis van de informatievoorziening. Dit betreft onder andere het standaardiseren en automatiseren van het software-voortbrengingsproces, het realiseren van de platformvisie en -strategie en het realiseren van Politienet 2.0 waarmee politiemedewerkers overal toegang moeten krijgen tot de IT-diensten in de cloud.[43] Het Programma Vernieuwend Registreren (PVR) heeft tot doel om de twaalf registratiesystemen – waaronder BVH[44] en Summ-IT[45] – te vervangen door één registratieve functionaliteit op basis van één onderliggend platform: het Operationeel Politie Platform (OPP).[46] Door gebruik te maken van moderne technologieën – zoals het verwerken van multimedia – moet dit vernieuwingsprogramma ook leiden tot een optimale ondersteuning van uitvoerende politiemensen in hun werk. De ontwikkeling naar het OPP zorgt ervoor dat het organiseren van data voor datagedreven politiewerk gemakkelijker wordt, onder andere omdat er gebruik wordt gemaakt van een gedeeld datamodel in uiteenlopende werkprocessen.[47]

---

38 Zie Van de Sandt et al. (2022) voor de verschillende lagen van harmonisatie die nodig zijn waarbij de ene laag randvoorwaardelijk is voor de andere laag. Om te komen tot technische harmonisatie is juridische en organisatorische harmonisatie nodig. Juridische harmonisatie verwijst naar wet- en regelgeving voor bijvoorbeeld het delen van data. Organisatorische harmonisatie heeft onder andere betrekking op de aanwezigheid van één nationaal beheerde politieorganisatie, wat in principe een goed uitgangspunt is voor technische harmonisatie (zie ook de paragraaf over organisatiemodel).

39 Roest 2023.

40 Linder 2019; Wilson 2019.

41 Egbert & Leese 2021: 288.

42 Ik richt me hierbij vooral op de ontwikkelingen van nieuwe platformen. Hierbij moet worden beseft dat technische harmonisatie meer omvat (zie Van de Sandt et al., 2022). Het gaat bijvoorbeeld ook om harmonisatie in datamodellen, waar onder andere Hyperion voor is bedoeld (zie hoofdstuk 18), en de wijze waarop wordt omgegaan met autorisatie.

43 Zie onder andere de IV-bijlage bij het eerste halfjaarbericht 2022 over de politie van de minister van Justitie & Veiligheid van 17 juni 2022.

44 BVH wordt vooral gebruikt in de basisteams (vooral artikel 8 Wpg-gegevens).

45 Summ-IT wordt vooral gebruikt door rechercheonderdelen (artikel 9 Wpg-gegevens).

46 Zie Deloitte 2020.

47 De huidige handmatige, vaak meervoudige, invoer moet daarnaast worden vervangen door eenmalige invoer met vooraf ingevulde informatie en intuïtief gebruik. Dit verkleint de kans op invoerfouten en moet dus bijdragen aan verbetering van de kwaliteit van data. Zie ook hoofdstuk 25 over 'datawerk'.

Naast platformisatie op het niveau van de registratiesystemen wordt er geïnvesteerd in platformen ten behoeve van het combineren van data uit uiteenlopende bronnen (ontsluitingssystemen).[48] Het gaat dat in de eerste plaats om het combineren van data uit verschillende registratiesystemen en andere bronnen ten behoeve van intelligence. Het datawarehouse op het gebied van cybercriminaliteit van het THTC voorziet hierin[49] én ook de ontwikkeling van Helios is hierop gericht (zie hoofdstuk 18). Een ander voorbeeld is het eerder behandelde sensing platform, waarin data uit verschillende soorten sensing-toepassingen op eenduidige wijze worden verwerkt (zie hoofdstuk 17). De hiervoor genoemde platformen zijn primair bedoeld om data te benutten voor – en in het politiewerk. Er zijn ook platformen die vooral zijn bedoeld om data beschikbaar te maken voor de ontwikkeling van big data en AI-toepassingen. Het gaat dan onder andere om het big data platform van de politie: het politie data platform (PDP).[50] Bij dit platform is het streven om data zo veel mogelijk los te koppelen van werkprocessen en systemen en eenmalig vast te leggen via gestandaardiseerde interfaces.[51] Het PDP is een belangrijke vernieuwing in de informatievoorziening van de politieorganisatie. Een van de toepassingen waarvoor het PDP wordt gebruikt, is het Advanced Analytics Platform (AAP).[52] Dit is een platform voor het ontwikkelen van machine learning applicaties. De softwareontwikkelaars, data engineers, data-analisten en datawetenschappers van de politie gebruiken dit platform onder andere voor het analyseren van data en trainen van (AI)-modellen (zie ook 'personeel').[53] Dit platform is onder andere gebruikt voor de ontwikkeling van de MONOcam (zie hoofdstuk 14).

Bovenstaande beschrijving is verre van volledig,[54] maar geeft wel een indruk van de ontwikkelingen die op het gebied van informatievoorziening gaande en ook nodig zijn om datagedreven politiewerk verder tot ontwikkeling te brengen. Op basis van empi-

48 Hierbij is er een onderscheid te maken tussen een datawarehouse waarin gestructureerde data worden opgeslagen en een data lake waarin ongestructureerde data worden opgeslagen. De politie gebruikt beide typen opslagfunctionaliteiten waarbij data lakes relatief nieuw zijn. Zie verder: Thamm, Gramlich & Borek 2020.

49 De Adviescommissie voor de landelijke eenheid (2022) ziet het komen tot één datawarehouse voor de landelijke eenheid als randvoorwaarde voor datagedreven werken binnen de landelijke eenheid. Het datawarehouse van het THTC moet hiervoor de basis zijn en het streven is om vanuit één datawarehouse voor de landelijke eenheid toe te werken naar één datawarehouse voor het hele korps. Hierbij moet naar mijn idee rekening worden gehouden met enigszins vergelijkbare ontwikkelingen die gaande zijn, waaronder Helios. Zie ook de paragraaf over het organisatiemodel.

50 Ik baseer me hierbij op vacatureteksten en op de jaarverantwoording van de politie. Zie bijvoorbeeld de jaarverantwoording van 2020.

51 Zie hiervoor Politie (2022). Deze manier van werken staat in de wereld van gemeenten bekend als Common Ground: een hervorming van de gemeentelijke informatievoorziening, door op een andere manier om te gaan met gegevens. Gegevens worden eenmalig vastgelegd en blijven bij de bron (zie eerder over de single source of truth) en worden opgehaald met zogenaamde API's: application programming interface. Een API maakt de overdracht van data van het ene naar het andere systeem mogelijk.

52 Zie https://reitsma.io/blog/aap (voor het laatst geraadpleegd op 28 december 2021). Zie ook deze video: https://www.youtube.com/watch?v=O5cCYXE1ufc&t=21s .

53 Organisaties die vooroplopen met datagedreven werken beschouwen het (snel) kunnen ontwikkelen en in productie kunnen nemen van (nieuwe) algoritmen als een werkproces of operatie. Dit wordt ook wel aangeduid met *machine learning operations* (zie bijvoorbeeld Davenport & Mittal, 2023).

54 In deel III van dit boek zijn verschillende praktijken behandeld die ook onderdeel zijn van platformisatie. Dit betreft onder andere de Raffinaderij en Hansken (hoofdstuk 13). Dit betreft meer specifieke platformen.

risch onderzoek in onder andere Duitsland, Zwitserland, Canada, het VK en de VS[55] heb ik de indruk dat de politie in Nederland in internationaal verband vooroploopt in de transitie van de informatievoorziening in het kader datagedreven werken.[56] Hierbij speelt mee dat de politie in Nederland al geruime tijd bezig is met landelijke uniformering.[57] De (technische) basis van de informatievoorziening is in de afgelopen tien jaar sterk verbeterd. Het applicatielandschap is geüniformeerd en het aantal applicaties is sterk teruggebracht. De vorming van een nationaal beheerde politieorganisatie heeft in dit proces geholpen.[58] Dit neemt echter niet weg dat de transitie van de informatievoorziening in het kader van datagedreven politiewerk complex is, lang duurt en met allerlei knelpunten gepaard gaat. Eind 2022 signaleerde de politie dat het risico aanwezig is dat de komende jaren niet alle ambities kunnen worden gerealiseerd in het tempo dat wenselijk wordt geacht.[59] Dit is ambtelijke taal om aan te geven dat de transitie vertraagt. De vernieuwing van de informatievoorziening vraagt daarnaast aanzienlijke financiële investeringen. Om een voorbeeld te geven: het PVR kost ongeveer vierendertig miljoen euro per jaar en duurt minimaal zeven jaar.[60] De ICT-begroting van de politie is in de afgelopen jaren dan ook flink gestegen waarbij de politie verhoudingsgewijs steeds meer is gaan uitgeven aan ontwikkeling.[61] Door deze verschuiving zijn er nu en in de komende jaren onvoldoende financiële middelen aanwezig voor het beheren van het totale ICT-landschap van de politie ('technische schuld').[62] Hierdoor ontstaat een risico dat zich bij allerlei organisaties die transformeren naar datagedreven werken voordoet: de kosten van de transformatie worden onderschat en het budget sluit niet aan bij de ambitie (of vice versa).[63] In een dergelijke context van financiele krapte is het van belang om te investeren in de (data)architectuur in plaats van in allerlei technologische innovaties die 'in het oog springen'.[64]

> *'The inner core of a business and the digital architecture is often the stronger competitive differentiator, even if that is not directly seen from the outside.'*[65]

55 Brayne 2021; Egbert & Leese 2021; Marciniak 2021; Sanders & Chan 2021.

56 De politie in Nederland heeft ook de ambitie om op het gebied van de digitale transformatie in de top van toonaangevende en innovatieve politiekorpsen te staan (zie Politie, 2022). Zie ook Testerink, Nieuwenhuizen & Bex (2023) die constateren dat de politie in Nederland – internationaal gezien – vooroploopt met AI.

57 Zie Mulder & Schönfeld 2023.

58 Zie ook De Kool, Vermeeren & Steijn (2023) over het voordeel van een gecentraliseerd politie apparaat met het oog op regie op de ontwikkeling van AI.

59 Zie de IV-bijlage bij het tweede halfjaarbericht 2022 over de politie van de minister van Justitie & Veiligheid van 14 december 2022.

60 PrincewaterhouseCoopers 2021.

61 Deze is normaliter ongeveer 70% beheer en 30% ontwikkeling. De politie voorziet dat op weg naar 2025 de verhouding verschuift naar 60%-40%. Zie PricewaterhouseCoopers (2021).

62 Idem.

63 Borek & Prill 2020.

64 Zie ook Ganesan (2022) die constateert dat investeren in de data-infrastructuur een belangrijke basis is waar een organisatie jaren op kan voortborduren.

65 Borek & Prill 2020: 19.

Tot slot moet worden opgemerkt dat er binnen de politie in Nederland twee werkelijkheden naast elkaar bestaan. Aan de ene kant loopt het korps – zoals eerder aangegeven – internationaal voorop in de transitie van de informatievoorziening in het kader van datagedreven werken. Aan de andere kant is de basis in verschillende opzichten nog niet op orde. Zo zijn veel processen nog niet gedigitaliseerd, wat onder andere impliceert dat er binnen de politieorganisatie en in de strafrechtketen nog een hoop papier rondgaat.[66] Dit is een belemmering voor de ontwikkeling naar datagedreven politiewerk.[67]

Personeel: nieuwe functies

De ontwikkeling naar datagedreven werken '…is as much about people as technology.'[68] Het vraagt allerlei investeringen in het 'menselijk kapitaal' van de organisatie. Dit betreft investeringen in zowel de kennis en vaardigheden van bestaande medewerkers als het aantrekken van nieuwe medewerkers in nieuwe functies.[69] In deze paragraaf staan deze (relatief) nieuwe functies centraal. Het gaat dan onder andere om AI-onderzoekers, softwareontwikkelaars, data-ingenieurs, datawetenschappers en data-analisten. Ik behandel wat deze functies op hoofdlijnen inhouden[70] en welke ontwikkelingen in de politieorganisatie gaande zijn.[71]

Om datagedreven werken verder te ontwikkelen, is wetenschappelijk onderzoek nodig. Het gaat dan in het bijzonder om onderzoek naar de mogelijkheden van AI voor het politiewerk en het – door middel van onderzoek – ontwikkelen van (concept)-AI-toepassingen. De politie in Nederland heeft in dit kader in 2019 een Nationaal Politielab AI opgericht waar onder andere promotieonderzoek wordt verricht.[72] Er zijn op dit moment ongeveer dertig fulltime medewerkers bij dit lab werkzaam, waaronder ongeveer vijftien promovendi van verschillende universiteiten.[73] Bij de dienst ICT van het Politiedienstencentrum gaat men toepassingsgericht verder met de uitkomsten van dit promotieonderzoek en onderzoekt men ook de meerwaarde van

66 Vanuit een bredere invalshoek kan bij 'de basis niet op orde' aan vele voorbeelden worden gedacht, zoals C2000.

67 Deze belemmering doet zich onder andere voor bij systemen die de kansrijkheid van zaken berekenen (zie hoofdstuk 10). Deze systemen hebben digitale zaaksdossiers nodig.

68 Davenport & Mittal 2023: 17.

69 Zie ook Ganesan 2022; Iansiti & Lakhani 2020; Thamm, Gramlich & Borek 2020.

70 Zie voor een nadere uitwerking van functies onder andere het handboek van Thamm, Gramlich & Borek 2020.

71 Ik beperk me in deze paragraaf tot de personeelssamenstelling. In hoofdstuk 25 ga ik in op de ontwikkeling van het vakmanschap van uitvoerende politiemensen.

72 Het Nationaal Politielab AI is een samenwerkingsverband tussen de politie, de Universiteit Utrecht en de Universiteit van Amsterdam. Het lab is onderdeel van het Innovation Center of Artificial Intelligence (ICAI): een nationaal netwerk van kennisinstellingen, bedrijfsleven en overheid op het gebied van AI. Het Nationaal Politielab AI illustreert een bredere ontwikkeling: de politie heeft in het kader van datagedreven politiewerk – en overigens ook ten behoeve van de aanpak van digitale criminaliteit – 'nieuwe vrienden' nodig en deze hebben meer dan voorheen het karakter van kennisinstellingen en private partijen.

73 Zie hiervoor het verslag van de bijeenkomst van de vaste Kamercommissie Digitale Zaken die heeft plaatsgevonden op 14 november 2022: https://www.tweedekamer.nl/kamerstukken/commissieverslagen/detail?id=-2022Z21400&did=2022D50031 (voor het laatst geraadpleegd op 3 januari 2023).

andere technologieën voor de operationele teams. Dit vindt plaats bij de afdeling 'Pre-Development' die inmiddels bestaat uit tientallen medewerkers die zich richten op onder andere AI.

Organisaties die datagedreven werken, ontwikkelen aan de lopende band slimme (AI)-software die hen helpt in de uitvoering van de taken. Dit is onderdeel van hun operationeel model en wordt mogelijk gemaakt door hun technische architectuur. Binnen de politie in Nederland vindt deze softwareontwikkeling op verschillende plekken plaats. Ontwikkeling en beheer van software zijn primair georganiseerd in het Productiehuis van de dienst ICT. Hier werken zo'n honderd DevOps-teams[74] die de platformen en applicaties van de politie (door)ontwikkelen en beheren en daarin samenwerken met de eindgebruikers.[75] Een deel van deze teams ontwikkelt en beheert platformen en applicaties ten behoeve van datagedreven politiewerk, zoals het eerdergenoemde AAP en de Raffinaderij (zie hoofdstuk 13). In deze multidisciplinaire teams werken *onder andere* diverse softwareontwikkelaars.[76] Multidisciplinaire teams die software ontwikkelen zijn tegenwoordig niet alleen te vinden binnen de dienst ICT. Deze bevinden zich ook in de operationele eenheden. Het THTC van de landelijke eenheid heeft een eigen Warehouse team. Dit team ontwikkelt software voor het THTC en de regionale cybercrime teams ten behoeve van de datagedreven aanpak van cybercriminaliteit. Het team bestaat uit politiemensen met een rechercheachtergrond, datawetenschappers, softwareontwikkelaars en platformspecialisten. Het team werkt mee aan grote (internationale) opsporingsonderzoeken en ondersteunt de operatie met het beantwoorden van onderzoeksvragen en aandragen van oplossingen op basis van datawetenschappelijke inzichten en methoden. Deze oplossingen worden vervolgens – wanneer mogelijk – beschikbaar gemaakt voor alle operationele (cybercrime)teams.[77] Daarnaast is er in een deel van de eenheden – zoals eerder aangegeven (zie hoofdstuk 13) – een Team Rendement Operationele Informatie (TROI). Deze multidisciplinaire teams ontwikkelen applicaties die door operationele medewerkers kunnen worden gebruikt om grote hoeveelheden data te analyseren. Tot slot zijn de innovatieteams binnen de politie – zoals de Q-LAB's – ook actief op het gebied softwareontwikkeling. Dit geldt in het bijzonder voor het innovatielab (iLab) in de eenheid Limburg dat over eigen softwareontwikkelaars beschikt.

74 DevOps staat voor de combinatie van development en operations. Dit is manier van softwareontwikkeling waarbij de ontwikkel- en beheeractiviteiten worden samengenomen. Dit verschilt van de meer traditionele manier van organiseren waarbij ontwikkeling en beheer (functioneel beheer, beveiliging, kwaliteit, et cetera) apart waren georganiseerd in verschillende afdelingen of teams. DevOps teams zijn dus tot op zekere hoogte multidisciplinaire teams (zie de paragraaf over het organisatiemodel).

75 Het Productiehuis heeft verschillende productielijnen waarin de DevOps-teams zijn ondergebracht. Zo is er een productielijn 'business intelligence' waar de Raffinaderij onder valt.

76 Hierbij wordt een onderscheid gemaakt tussen ontwikkelaars die aan de code en datastructuur van een applicatie werken (back-end) en ontwikkelaars die aan de gebruikersinterface werkt (front-end). De combinatie van beide wordt 'full-stack' genoemd.

77 Zie ook Kroes, Ter Veen & Kop 2023.

Om de benodigde randvoorwaarden voor datagedreven politiewerk en de huidige situatie binnen de politie in Nederland beter te begrijpen, is het van belang om nader in te gaan op de 'datafuncties' die nodig zijn voor datagedreven werken.[78] Ik begin met de data-ingenieur (*data engineer*). Deze heeft verstand van datastructuren en databases en richt zich vooral op de infrastructurele-technische kant van datagedreven politiewerk. Het gaat dan onder andere om het ophalen (via 'data pijplijnen', API's), opschonen en integreren van data, zodat het voor anderen bruikbaar wordt. Deze anderen zijn onder andere datawetenschappers die de geprepareerde data gebruiken voor het trainen van hun modellen. Dat brengt me bij de functie van datawetenschapper (*data scientist*). Een datawetenschapper heeft verstand van statistiek, AI en programmeren en houdt zich vooral bezig met de modelmatige kant van datagedreven politiewerk (zie ook hoofdstuk 5). Dit betreft vooral het (door)ontwikkelen van algoritmen.

Een voorbeeld: datawetenschapper Dennis[79]

Het CAS is mede ontwikkeld door Dennis, die als datawetenschapper bij de politie werkt. Dennis is afgestuurd in de mathematische psychologie. Hij heeft ruime werkervaring opgedaan als statisticus bij twee universiteiten en daarna gewerkt in de farmaceutische industrie en reclamebranche (als *data-miner)*.[80] Hij wilde zijn data- en modelleerexpertise in een maatschappelijke context inzetten en besloot in 2012 te solliciteren voor de functie van data scientist bij de politie in Amsterdam. Dennis was geïnspireerd geraakt door het PredPol algoritme in de VS en wilde een dergelijke vorm van predictive policing ook in Nederland ontwikkelen (zie hoofdstuk 19). Dennis ging er – als hoofdontwikkelaar van het CAS – vanuit dat het identificeren van patronen in crimineel gedrag op een vergelijkbare manier kon worden gedaan als bij klantomzet in de reclame-industrie. Met behulp van datamining heeft hij in data over criminaliteit gezocht naar patronen. Die patronen zijn vervolgens gebruikt voor het bepalen van relevante variabelen en hun gewicht. Dennis heeft samen met zijn collega-datawetenschappers allerlei keuzes moeten maken met betrekking tot ander andere de data die worden gebruikt, de wijze van verwerken (neuraal netwerk is aangepast in een logistische regressie), de categorisering en weging van variabelen en de wijze waarop de uitkomsten worden gepresenteerd. Deze keuzes maken duidelijk dat datawetenschappers (veel) invloed hebben op de totstandkoming van zelflerende algoritmen (zie ook het volgende hoofdstuk).

78 Zie bijvoorbeeld Borek & Prill 2020; Rashedi 2022.

79 Deze passage is volledig gebaseerd op Van Waardenburg, Sergeeva & Huysman 2020.

80 Datamining kan worden beschouwd als een voorloper van datawetenschap en is nu een techniek binnen de datawetenschap (zie Den Hengst & Wijsman, 2023). Datawetenschap is – zoals eerder aangegeven (hoofdstuk 5) – de bredere paraplu waar ook AI onder valt.

De politie in Nederland is tien jaar geleden begonnen met het aannemen van enkele datawetenschappers.[81] Anno 2023 zijn er in totaal meer dan 100 datawetenschappers bij de politie werkzaam.[82] Datawetenschappers, maar ook data-ingenieurs, werken binnen verschillende organisatieonderdelen. Het gaat dan vooral om de afdelingen en teams die software ontwikkelen en beheren, de intelligenceorganisaties van de eenheden en de teams digitale opsporing van de recherche. De software – waarvan de algoritmen een onderdeel zijn – wordt in de regel gebruikt door *data-analisten* die gegevens analyseren in en ten behoeve van het politiewerk. De functie van analist is binnen de intelligenceorganisatie van de politie al langer aanwezig, maar deze analist moet in toenemende mate kunnen omgaan met geavanceerde software en de werking van deze software ook enigszins kunnen begrijpen. Daarnaast zijn er in toenemende mate data-analisten nodig in andere domeinen, in het bijzonder binnen de tactische recherche. Tot slot moet worden opgemerkt dat software ook in toenemende mate wordt gebruikt door 'generalisten', waaronder tactisch rechercheurs. De missie van TROI is hier expliciet op gericht (zie hoofdstuk 13).

Het voorgaande geeft een indruk van de veranderingen die in de personeelssamenstelling van de politie nodig zijn om datagedreven te kunnen werken. De uiteenzetting maakt tevens duidelijk dat de politie volop investeert in veranderingen in de personeelssamenstelling. In de afgelopen jaren zijn er in het kader van datagedreven politiewerk – naar mijn indruk – honderden nieuwe experts de politieorganisatie ingestroomd en deze ontwikkeling is nog volop gaande.[83] Hierbij staat de politie voor de uitdaging om het gat te dichten tussen medewerkers met kennis van AI en medewerkers in de operatie.[84] Dit vraagt niet alleen van de nieuwe experts dat zij zich verdiepen in het politiewerk, maar ook van uitvoerende politiemensen dat zij zich verdiepen in datagedreven werken. In hoofdstuk 25 ga ik hier nader op in onder de noemer van politievakmanschap.

Organisatiemodel: hybride structuren

De secundaire (ondersteunende) functie van technologie is binnen de politie – zoals eerder aangegeven – aan het veranderen in een primaire functie. Technologie beweegt zich van de randen van het politiewerk naar de kern. Een politie die datagedreven wil werken, moet zich tot op zekere hoogte ontwikkelen tot een technologie-organisatie.[85] Organisaties die deze transformatie hebben ondergaan en excelleren in datage-

81 Den Hengst & Wijsman 2023.

82 Dit baseer ik op een LinkedIn bericht (juni 2023) waarin de vacature voor een coördinator vakontwikkeling (senior datawetenschapper) werd gedeeld.

83 Ik heb voor deze paragraaf gebruikgemaakt van tientallen vacatureteksten die ik heb verzameld (zie ook Schuilenburg & Soudijn, 2021 voor deze werkwijze). Het is van belang op te merken dat het naast de behandelde functies ook gaat om *onder andere* machine learning platform engineers (die werken aan het eerder behandelde PDP en vooral aan het AAP), spraaktechnologen, juridisch adviseurs op het gebied van AI en adviseurs AI ethiek (zie ook hoofdstuk 29).

84 Roest 2023; zie ook Waardenburg, Sergeeva & Huysman 2020.

85 Zie in meer algemene zin: Daugherty & Wilson 2022.

dreven werken hebben veelal een organisatiemodel dat in de eerste plaats wordt gekenmerkt door het hand in hand gaan van centralisatie en decentralisatie.[86] Er vindt centrale sturing plaats op onder andere investeringen in use cases, gedeelde standaarden, infrastructuren en voorzieningen (o.a. platformen).[87] Naast centralisatie in sturing en organisatie is er sprake van decentralisatie: wendbare teams die dicht op het primaire proces experimenteren met datagedreven oplossingen. In deze organisaties worden centralisatie en decentralisatie én koersvast en wendbaar als aanvullend aan elkaar in plaats van contrair met elkaar beschouwd:

> *'What is more important – agility or discipline? This is a misleading question, as agility requires a lot of discipline and focus to succeed. Discipline is needed to stick to a business vision and the organizational set-up keeping it stable for a long time so agile teams can actually perform. Discipline is also necessary to focus on a well-managed portfolio of data products, capabilities and change activities that follow the priorities set in the data and AI strategy and transformation roadmap. This prevents spreading the resources and attention of agile teams out too thinly and losing track of what is important.'*[88]

De nationale politieorganisatie biedt een goed uitgangspunt voor centrale sturing op gedeelde standaarden, infrastructuren en technologieën. Hoewel er op dit punt het nodige is bereikt – zie de paragraaf over de informatievoorziening – functioneert de centrale sturing binnen de politie zeker niet optimaal. Eind 2017 concludeerde de Commissie Evaluatie Politiewet 2012 dat het gecentraliseerd, op *leane* wijze willen sturen van de politie – in een land dat verdeelde macht en collegiaal bestuur in haar genen heeft – niet meer dan een romantisch verlangen is.[89] De pogingen tot centrale sturing gaan geregeld gepaard met allerlei 'tegenkrachten' en intensief overleg in allerlei gremia. Deze tegenkrachten zijn soms functioneel, omdat deze zorgen voor evenwicht. Voor het realiseren van gedeelde standaarden, infrastructuren en voorzieningen zijn de tegenkrachten naar mijn indruk vaker disfunctioneel, omdat deze resulteren in een gebrek aan daadwerkelijke richting en discipline in de realisatie. De benodigde (technische) harmonisatie lijdt hieronder en concurrentie tussen de verschillende ontwikkelingen en organisatieonderdelen kost veel (onnodige) inspanningen, doorlooptijd en financiële middelen.[90]

Dan de andere kant van de medaille: decentraal experimenteervermogen. Dit is binnen de politie in Nederland volop aanwezig. Er zijn naast de centraal geïnitieerde vernieuwingsoperaties – zie ook de volgende paragraaf – allerlei (technologische) innovaties die op decentraal niveau worden geïnitieerd door innovatieteams en -hubs. Het op-

86 Borek & Prill 2020; Iansiti & Lakhani 2020; Rashedi 2022; Thamm, Gramlich & Borek 2020.
87 Iansiti & Lakhani 2020
88 Borek & Prill 2020: 237.
89 Commissie Evaluatie Politiewet 2012 2017.
90 Zie Kroes, Ter Veen & Kop 2023.

schalen van deze decentraal geïnitieerde technologische innovaties naar de gehele organisatie verloopt echter moeizaam.[91] Dit heeft verschillende redenen, die voor een deel zijn terug te voeren op een mismatch tussen het besturingsmodel van de politie en het decentrale experimenteervermogen.[92] Het besturingsmodel bestaat onder andere uit een portfolioproces voor investeringskeuzes.[93] Dit proces is onvoldoende toegesneden op technologische innovaties die bottom-up ontstaan. Dit heeft gevolgen voor de mate waarin dergelijke innovaties binnen het portfolio prioriteit krijgen en worden ondersteund met financiële middelen en de benodigde capaciteit op het gebied van informatievoorziening.[94] Hierbij speelt mee dat het inhoudelijke kader waarbinnen technologische innovaties moeten plaatsvinden onvoldoende disciplinerend is. Dit punt is bij strategie ook behandeld: er is onvoldoende scherpte in de use cases die prioriteit krijgen dan wel hier wordt onvoldoende op gestuurd. Hierdoor investeren de wendbare (innovatie)teams soms tijd en geld in het (te ver) ontwikkelen van technologische innovaties die in het geheel – zodra opschaling in zicht komt – minder belangrijk worden gevonden door de beslissers.

Kortom: de politie vindt het lastig om centralisatie en decentralisatie hand in hand te laten gaan. Ik herhaal een deel van het eerder opgenomen citaat: 'Discipline is needed to stick to a business vision and the organizational set-up keeping it stable for a long time so agile teams can actually perform.' Het is juist deze discipline die (soms) ontbreekt, wat maakt dat het decentrale experimenteervermogen minder oplevert dan zou kunnen. Een van de gevolgen van de onvolkomen centralisatie en de ongerichte decentralisatie is dat het de politie moeite kost om de stap te zetten van technologiegebruik op kleine schaal naar gebruik op grote schaal. Het proces van technologisch innoveren – van idee tot brede implementatie – heeft binnen de politieorganisatie gemiddeld genomen dan ook een lange doorlooptijd.[95]

Een tweede kenmerk van organisaties die excelleren in datagedreven werken is dat zogenaamde *cross-functional teams* werken aan datagedreven oplossingen.[96] Dit zijn teams die bestaan uit medewerkers met verschillende typen expertise. In het organisa-

91 Idem. De politie is hierin overigens (zeker) niet uniek. Davenport & Mittal (2023) wijzen erop dat organisaties die data- of AI-gedreven zijn een breed scala aan AI-toepassingen in productie hebben. In de praktijk hebben veel organisaties veel van hun toepassingen in een proof of concept fase en kost het veel moeite om organisatiebreed te implementeren.

92 In de literatuur over innoveren wordt erop gewezen dat organisaties die structureel willen vernieuwen, moeten beschikken over 'tweehandigheid'. Hiermee wordt bedoeld dat er gelijktijdig uitvoering wordt gegeven aan twee type processen: exploiteren (bestaande incrementeel verbeteren) en exploreren (radicaal vernieuwen). Organisaties die hier goed in slagen, worden 'ambidextere organisaties' genoemd (zie bijvoorbeeld Mandour, Van der Heijden & Turnhout, 2020). Voor de politie geldt dat veel processen meer zijn afgestemd op exploiteren dan op exploreren. Dit bemoeilijkt innoveren, in het bijzonder in de fase van opschaling.

93 Zie Mulder & Schönfeld (2023) die ingaan op het 'portefeuillesysteem' binnen de politie en de daarmee samenhangende ingewikkelde besluitvorming.

94 Zie Ernst et al. 2019; Kroest, Ter Veen & Kop; Mulder & Schönfeld 2023.

95 In een longitudinaal onderzoek naar dertien technologieprojecten is er sprake van een gemiddelde looptijd van zo'n negen jaar (Ter Veen & Kop, 2021).

96 Borek & Prill 2020; Fountaine, McCarthy & Saleh 2019.

tiemodel wordt tevens voorzien in de verbinding tussen medewerkers met dezelfde expertise. In dit verband wordt er geregeld verwezen naar organisatiemodellen als dat van Spotify met onder andere *squads, tribes, guilds* en *chapters*.[97] In dergelijke 'wendbare' organisatiemodellen wordt onder andere getracht de spanning tussen het inrichten van de organisatie op basis van disciplines of vakgebieden en het inrichten van de organisatie op basis van producten of opgaven op effectieve wijze te hanteren. Het zogenaamde Spotify-model bestaat in essentie uit multidisciplinaire teams die werken aan de producten of opgaven en uit guilds en chapters die zijn geordend op basis van expertisegebieden. Deze guilds en chapters zijn ook te beschouwen als teams. Hiermee kom ik op een kenmerk van veel 'moderne' organisaties. Teams zijn in dergelijke organisaties niet langer de stabiele entiteiten die onderdeel zijn van de organisatiestructuur. Teams hebben een vloeiend karakter waarbij specialisten in- en uitvoegen op basis van wat de gezamenlijke opgave vraagt.[98] Als medewerker ben je lid van meerdere teams tegelijk.[99] Het draait niet zozeer om teams, maar om *teaming*: het vermogen om over de grenzen van teams, afdelingen, bedrijfseenheden en ook disciplines heen samen te werken om zo meer te leren, sneller te innoveren en beter te presteren.[100]

De dominante ordening van de politieorganisatie is functioneel.[101] Dit wil zeggen dat mensen met vergelijkbare taken en vakgebieden bij elkaar zijn gebracht in de onderdelen van de organisatiestructuur (teams, afdelingen, sectoren). Deze inrichtingskeuze heeft als gevolg dat de voornaamste opgave is gelegen in het organiseren van de multidisciplinaire werksystemen die samenwerken aan het ontwikkelen of uitvoeren van datagedreven manieren van werken.[102] Hierbij kan worden gedacht aan generalisten, digitaal specialisten, data-engineers, datawetenschappers, data-analisten en (eventuele) andere specialisten die met elkaar samenwerken aan het ontwikkelen of uitvoeren van datagedreven manieren van werken.[103] Binnen de politie is de ontwikkeling naar meer dynamische teams – dwars op de organisatiestructuur – gaande. Een voorbeeld hiervan is het eerder behandelde TROI dat als 'netwerkonderneming' binnen de politie functioneert.[104] Daarnaast kan worden gedacht aan het – in ontwikkeling zijnde – hub-and-spokes-model voor de datawetenschappers binnen de politie.[105] De (vooral) decentraal geplaatste datawetenschappers werken via een netwerkstructuur samen aan de ontwikkeling van het vakgebied. Zo zijn er meer voorbeelden.[106] De goede voor-

97 Zie bijvoorbeeld Borek & Prill 2020; Thamm, Gramlich & Borek 2020.
98 Edmondson 2012.
99 Ruijters 2017.
100 Van der Loo & Davidson 2022.
101 Landman, Kouwenhoven & Brussen 2020.
102 Den Hengst & Wijsman 2023; Roest 2021.
103 Van de Sandt et al. 2022; zie ook Den Hengst & Wijsman 2023; Klerks & Vink-Teeven 2020.
104 Zie Roest 2021.
105 Dit wordt de *Hub voor Advanced Analytics & AI* genoemd. Zie verder: Den Hengst & Wijsman 2023. Zie in meer algemene zin over dit model in het kader van AI: Rashedi 2022; Thamm, Gramlich & Borek 2020.
106 De eerder behandelde Dev-Op teams zijn tot op zekere hoogte ook te beschouwen als cross-functionele of multidisciplinaire teams. Met de komst van deze teams worden gebruikers meer bij softwareontwikkeling betrokken (zie ook Mulder & Schönfeld, 2023).

beelden zijn echter de uitzonderingen op de regel. Het kost veelal moeite om vanuit de functionele kolommen van de organisatiestructuur samen te werken aan gezamenlijke opgaven,[107] waaronder technologische innovaties.[108] Hierbij speelt mee dat de bedrijfsvoering (formatie, budget) aan de organisatiestructuur is 'opgehangen'.[109] Anders gezegd: bevoegdheden en middelen zijn afgestemd op de stabiele entiteiten (stabiliteitssysteem) en niet op de meer fluïde teams (werksystemen).

Op basis van het voorgaande kom ik tot de conclusie dat datagedreven organisaties in staat zijn om in hun organisatiemodel verschillende principes naast elkaar te hanteren, waaronder centraal én decentraal en organiseren op basis van opgave én organiseren op basis van taak/expertise. Dit kost de politieorganisatie vooralsnog moeite. Oplossingen worden dan gezocht in het versterken van het ene of het andere. Tegenwoordig wordt er vooral gepleit om afscheid te nemen van de huidige hiërarchische organisatiestructuur en een horizontale, bottom-up structuur te omarmen.[110] Dergelijke pleidooien gaan naar mijn idee voorbij aan een belangrijke essentie: het gaat niet om kiezen voor het een of het ander, maar om het hanteren van de spanning ertussen.

Cultuur: nieuwe manier van werken
Datagedreven werken is volgens de (organisatie)literatuur ook een culturele opgave. Deze opgave heeft betrekking op uiteenlopende aspecten, waaronder de eerdergenoemde samenwerking tussen verschillende disciplines. In deze paragraaf wordt een van de belangrijkste aspecten of deelopgaven behandeld: adoptie van datagedreven technologie in het algemeen en AI in het bijzonder op een manier die vernieuwing in de manier van werken brengt. Experts op het gebied van organisatieontwikkeling en AI constateren dat AI in organisaties vooralsnog meer wordt gebruikt binnen de bestaande manier van werken (*point solutions*) dan om de manier van werken wezenlijk te vernieuwen (*system solutions*).[111] Dit is volgens hen kenmerkend voor de *between times* waarin AI zich nu bevindt: na grootschalige adoptie en voor de benutting van diens 'ware' potentieel (zie hoofdstuk 5). De stap van inpassing binnen bestaande manieren van werken naar benutting voor het ontwikkelen van vernieuwende manieren van werken is echter niet zomaar gezet.[112]

Datagedreven werken maakt binnen de politie nieuwe manieren van werken mogelijk. Ik geef enkele voorbeelden. Door gebruik te maken van veiligheidsanalyses kan de politie probleemgerichter werken aan de aanpak van georganiseerde criminaliteit, door gebruik te maken van cryptocommunicatiedata kan de politie met minimale inzet van bijzondere opsporingsbevoegdheden tot afronding van opsporingsonderzoe-

107 Zie ook Landman, Kouwenhoven & Brussen 2020.
108 Ernst et al. 2019.
109 Zie Roest 2021.
110 Den Hengst & Wijsman 2023; Roest 2021.
111 Agrawal, Gans & Goldfarb 2022.
112 In dat opzicht hebben start-ups het gemakkelijker dan bestaande (grote) organisaties.

ken komen, door gebruik te maken van predictive mapping kan de politie gerichter capaciteit inzetten en surveilleren én door gebruik te maken van mobiele identificatietechnologie kan de politie beter gepleegde misdrijven reconstrueren. Anders gezegd: het gebruik van opkomende technologieën kan leiden tot vernieuwing in de manier waarop politiewerk wordt uitgevoerd.

Het schaarse, empirische onderzoek naar technologie-adoptie in de politieorganisatie maakt echter duidelijk dat het gebruik van opkomende technologieën – net als in veel andere, grote organisaties – vooral wordt ingepast binnen de al bestaande manier van werken.[113] Dit komt naar voren uit (evaluatie)onderzoek naar predictive mapping[114] en mobiele identificatietechnologie[115] in Nederland en wordt (indicatief) bevestigd door praktijkervaringen die in deel III van dit boek zijn behandeld. Onderzoek uit het VK en de VS toont hetzelfde beeld.[116] Bestaande patronen in de uitvoering van politiewerk zijn stevig in de politieorganisatie ingebed. Technologie is niet deterministisch. Het dwingt geen vernieuwing af. Die vernieuwing komt al dan niet tot leven in sociale praktijken; door handelingen van verschillende actoren in hun context.[117] Dit maakt technologie-adoptie binnen de politie weerbarstig en qua uitkomsten ook enigszins onvoorspelbaar.[118]

Deze weerbarstigheid wordt vooral veroorzaakt door de dominante manier waarop uitvoerende politiemensen en hun direct leidinggevenden naar het politiewerk kijken; hun *cultural frames*.[119] Deze manier van kijken is van invloed op de adoptie van nieuwe technologie.[120] Om het concreet te maken: als politiemensen het reageren op incidenten als de essentie van het straatwerk zien, dan zullen zij ook op deze wijze naar het gebruik van nieuwe technologie kijken. Als politiemensen het verzamelen van informatie door middel van opsporingsmethoden als de essentie van het recherchewerk zien, dan zullen zij ook op deze wijze naar het gebruik van nieuwe technologie kijken. De rode draad in de oriëntatie van uitvoerende politiemensen is dat zij zich meer richten op het operationele gebruik op de korte termijn – maakt het de huidige manier van uitvoeren nu gemakkelijker? – dan op het strategisch gebruik op de langere termijn: kunnen we hiermee straks tot nieuwe manieren van werken komen?[121] Het risico bestaat dat dominante, decennialang bestaande, patronen in het politiewerk als gevolg van technologiegebruik eerder worden versterkt dan doorbroken.[122] Peter Manning

113 Zie voor algemene studies: Egnoto et al. 2017; Lum, Koper & Willis 2017.
114 Mali, Bronkhorst-Giesen & Den Hengst 2017.
115 De Gruijter, De Poot & Elffers 2016; De Gruijter 2017; Mapes 2017.
116 Brayne 2021; Ferguson, 2017a; Hestehave, 2018; Lum, Koper & Willis 2017; Manning, 2008; McDaniel & Pease 2021b; Willis, Koper & Lum 2022.
117 Brayne 2021.
118 Terpstra & Salet 2020; Willis, Koper & Lum 2022.
119 Ratcliffe et al. 2021.
120 Koper & Lum 2019; zie ook Dewald 2023.
121 Koper et al. 2014; Ernst et al. 2019.
122 Ferguson 2017a; McDaniel & Pease 2021b; Willis et al. 2022.

formuleert het treffend: 'Organizations do what they have done well in the past.'[123] Dit is een knelpunt als vernieuwing van politiewerk het streven is.

Bij het voorgaande speelt mee dat uitvoerende politiemensen nieuwe technologieën kunnen ervaren als een bedreiging voor hun professionele identiteit (zie ook hoofdstuk 24).[124] Datagedreven politiewerk gaat, zoals eerder aangegeven (zie hoofdstuk 22), gepaard met een verandering in de wijze waarop kennis wordt geproduceerd. De professionele intuïtie verliest aan terrein ten gunste van datawetenschappelijke methoden. Dit doet afbreuk aan het zelfbeeld van de autonome en intuïtieve politieprofessional. Het geeft politiemensen het gevoel dat hun ervaringskennis wordt gedevalueerd of wordt aangetast. Dit baart hen zorgen.[125] Deze sociale processen creëren niet alleen weerstand tegen de introductie van nieuwe technologieën in het politiewerk, maar kunnen er ook toe leiden dat men de technologie niet gebruikt of anders gebruikt dan de bedoeling is in het kader van vernieuwing van politiewerk.[126] Dit bemoeilijkt de beoogde technologie-adoptie.

De opgave is om technologische en sociale innovatie hand in hand te laten gaan.[127] Vanaf de start van de technologieontwikkeling dienen de gewenste veranderingen in de manier van werken te worden meegenomen.[128] Het gaat dan dus niet alleen om het operationele gebruik van technologie, maar ook en vooral om het strategische gebruik.[129] Bijvoorbeeld: bij het ontwikkelen van een applicatie voor veiligheidsbeelden (Helios) is het essentieel dat de wijze waarop met deze beelden moet worden gewerkt en gestuurd, wordt meegenomen. Anders is de kans te groot dat technologie wordt geïmplementeerd binnen een bestaande manier van werken en daarmee onvoldoende tot diens recht of potentie komt. In dit geval komt probleemgericht werken dan niet van de grond. Onderzoek naar sociaal-technologische innovatie in het bedrijfsleven wijst uit dat het her-verbeelden – *reimagine* – van werkprocessen essentieel is om te komen tot daadwerkelijke vernieuwing.[130] De samenwerking tussen mens en machine is bij dit her-verbeelden een belangrijk onderdeel.

123 Manning 2008: 253.
124 Brayne 2021; Ratcliffe, Taylor & Fisher, 2020; zie ook De Kool et al. 2020 over het aangifteproces.
125 Ratcliffe, Taylor & Fisher 2020.
126 Zie bijvoorbeeld Böing 2013. Deze weerstand is overigens niet uniek voor de politie. Zie bijvoorbeeld Ganesan 2022.
127 Van den Broek et al. 2020; Volberda, Heij & Bosma 2019.
128 Daarom wordt ook wel gesteld dat een onderscheid tussen technologieontwikkeling enerzijds en organisatieverandering anderzijds in het tijdperk van AI steeds minder zinvol en bruikbaar is. Zie hiervoor Waardenburg (2021).
129 Lum, Koper & Willis 2017.
130 Daugherty & Wilson 2018; Davenport & Mittal 2023.

'To achieve substantial value from AI, a company should fundamentally rethink the way humans and machines interact in working environments.'[131]

Het her-verbeelden van werkprocessen is naar mijn idee een belangrijke opgave voor de politieorganisatie. Dit wil zeggen: loskomen van de bestaande routines en met verbeeldingskracht werken aan het ontwikkelen van nieuwe manieren van werken.[132] Anders kijken, anders denken en anders doen.[133] Alleen dan kan de potentie van de opkomende technologieën die zich nu aandienen ten volle worden benut.

131 Davenport & Mittal 2023: 10.

132 Een rode draad in dit proces van *reimagine* is dat AI kan bijdragen aan het meer parallel – in plaats van sequentieel – uitvoeren van werkprocessen. Hierbij kan in het kader van dit boek onder andere worden gedacht aan het integreren van tactisch en forensisch onderzoek doordat uitkomsten van DNA-onderzoek veel eerder in het proces beschikbaar (kunnen) komen (hoofdstuk 11) én aan het bij elkaar brengen van veiligheidsbeeld en interventiestrategie (hoofdstuk 18).

133 Zie Van Gelder 2022.

24 Politiewerk

In de voorgaande hoofdstukken is vanuit verschillende perspectieven gekeken naar de gevolgen van de voortschrijdende digitalisering in de samenleving voor de politie. Ik heb betoogd dat er virtualisering en technologisering van de politiefunctie plaatsvinden. De technologisering leidt binnen de politie tot een substantiële uitbreiding van met name het politiële vermogen tot waarnemen en informatie verwerken. Dit maakt (mede) een nieuw politiemodel mogelijk: datagedreven politiewerk. Om dit politiemodel in de praktijk te brengen, zijn er verschillende organisatorische randvoorwaarden nodig waaraan binnen de politie in Nederland wordt gewerkt. In dit hoofdstuk staat het politiewerk centraal. De stelling van dit hoofdstuk is dat er wezenlijke verschuivingen in het politiewerk gaande zijn. Deze verschuivingen impliceren dat enkele dominante beelden of kenmerken van politiewerk – straatwerk, reactief werk, lokaal ingebed werk en discretionair werk – minder relevant worden en er (dus) aanvullende beelden nodig zijn. Deze aanvullende beelden worden in dit hoofdstuk behandeld.

Meer politiebureauwerk

Het dominante beeld van het politiewerk in politieonderzoek,[1] politiek en maatschappij is het politiewerk op straat. Bij algemene uitspraken over het politiewerk wordt er vaak – al dan niet impliciet – gerefereerd aan het straatwerk; alsof politiewerk samenvalt met het straatwerk. Mijn verwachting is dat de ontwikkelingen die in dit boek zijn beschreven tot gevolg hebben dat het beeld van politiestraatwerk minder accuraat wordt als dominant beeld van politiewerk. Het politiewerk krijgt verhoudingsgewijs meer het karakter van bureauwerk. Dit heeft een aantal redenen.

De eerste reden heeft te maken met het veranderende veiligheidsvraagstuk (zie deel II). Criminaliteit en onveiligheid hebben in toenemende mate een digitaal karakter en manifesteren zich online. De politiefunctie en het politiewerk op het internet zullen zich de komende jaren verder ontwikkelen (zie ook hoofdstuk 20).[2] Dit leidt verhoudingsgewijs tot meer bureauwerk, omdat de aanpak van digitale criminaliteit en online

1 Zie ook Brodeur 2010; Hoogenboom 2009.

2 Een interessante vraag is of er ook een digitale noodhulpfunctie gaat ontstaan. Vooralsnog worden er wel aangiften van digitale criminaliteit opgenomen, maar is er geen brede functionaliteit om op meldingen van digitale criminaliteit en eventuele andere incidenten te reageren (zie ook Boekhoorn, 2019). Het gaat dan onder andere om beschikbaarheid bij incidenten van digitale criminaliteit voor onder andere het uitbrengen van handelingsadvies in dreigende situaties en het veiligstellen van sporen. Mocht een dergelijke functionaliteit worden ingericht, dan ligt een regionale of landelijke organisatie voor de hand, al dan niet in de vorm van publiek-private samenwerking (zie ook Kort & Spithoven, 2021).

aanwezigheid/gegevensvergaring vooral bestaan uit activiteiten die achter een computer worden uitgevoerd. Dat is ook zichtbaar in (relatief) nieuwe rollen als digitaal rechercheurs, digitaal wijkagenten, open source intelligence specialisten, webcare medewerkers, virtual agents, runners van informanten op het gebied van cybercriminaliteit en ga zo maar door. De politiemedewerkers die deze rollen vervullen, hebben in belangrijke mate een bureaubaan.

De tweede reden heeft te maken met datagedreven politiewerk. Voor datagedreven politiewerk zijn data logischerwijs essentieel. Dit betreft uiteenlopende data waaronder de dataproductie die is verweven met uitvoerend politiewerk (zie ook hoofdstuk 25).[3] De noodzaak om in het politiewerk data te verzamelen en deze goed vast te leggen, neemt in het tijdperk van datagedreven politiewerk (verder) toe.[4] Dit geldt voor het politiewerk in de basisteams, maar zeker ook voor rechercheonderdelen waar vooralsnog veel meer data worden verzameld dan in het bedrijfsprocessensysteem terechtkomen. Het verzamelen en vastleggen van data is niet alleen van belang voor allerlei intelligencedoeleinden, maar ook om AI beter te laten functioneren: *feeding the machine*.[5] Dit is onder andere zichtbaar bij de DNA-succesmeter: deze big data-software zou veel beter functioneren als er meer en beter wordt geregistreerd (zie hoofdstuk 11). Ik verwacht dat dergelijke registratiebehoeften in de politieorganisatie verder gaan toenemen, zodat (beter) datagedreven werken mogelijk wordt. Het gaat hierbij niet alleen om de basisregistraties, maar ook om het – in voorkomende gevallen – toekennen van labels aan data (classificeren). Kortom: politiewerk wordt meer datawerk en dit werk vindt deels vanachter het bureau plaats.

De derde reden voor relatief meer bureauwerk en minder straatwerk is sensorsurveillance: de surveillance door politiemensen op straat wordt in toenemende mate aangevuld en deels overgenomen door sensoren. Naarmate het netwerk van sensoren in de samenleving zich uitbreidt, kan er steeds meer worden waargenomen via technologie en is surveillance van de politie op straat minder nodig. Dit wil vanzelfsprekend niet zeggen dat de aanwezigheid van de politie op straat niet meer relevant of van meerwaarde is, want deze heeft meer doeleinden dan surveillance. Waar het (hier) om gaat, is dat deze noodzaak steeds minder te maken heeft met surveillance. Er zijn daarentegen steeds meer politiemensen nodig die in intelligence centers of rooms het politiewerk aansturen op basis van de data die vanuit het surveillancenetwerk binnenkomen.

De vierde reden hangt deels samen met de voorgaande redenen: de politie genereert *verhoudingsgewijs* steeds minder data via eigen activiteiten op straat. Neem de opsporing als voorbeeld: de politie genereert van oudsher data door bijvoorbeeld telefoonlijnen af te tappen, vertrouwelijke communicatie op te nemen (OVC) of op straat te ob-

3 Waardenburg 2021.
4 Zie ook Ferguson 2017a; Waardenburg, Huysman & Agterberg 2020.
5 Joh 2017.

serveren. Er waren geen data, maar deze worden door de politie gecreëerd. En deze creatie vindt voor een deel op straat plaats. Deze datacreatie wordt binnen de recherche ook wel 'in de actualiteit werken' genoemd. Deze manier van werken heeft op (een deel van de) rechercheurs aantrekkingskracht: zelf informatie verzamelen met aantrekkelijke, spannende opsporingsmethoden, als het even kan op straat.[6] De politie hoeft echter steeds minder data zelf te genereren. De data zijn er al: op servers, in computers, in smartphones en in toenemende mate ook in allerlei andere apparaten als onderdeel van de IoT. De politie neemt apparaten en servers in beslag, hackt apparaten[7] en past andere vormen van interceptie toe en krijgt zo enorme hoeveelheden data tot haar beschikking. De cryptocommunicatiedata zijn illustratief voor deze ontwikkeling naar meer *found data*. De politie heeft deze data niet gegenereerd en hoefde er niet of nauwelijks de straat voor op. De nadruk komt steeds meer op analyse te liggen (zie ook hoofdstuk 25).[8] Achter het bureau.

Meer proactief politiewerk

Het politiewerk is op dit moment sterk reactief:[9] de politie treedt op als er iets is gebeurd. De focus ligt op het verleden. Mijn verwachting is dat het politiewerk in de komende jaren – mede als gevolg van datagedreven werken – opschuift van sterk reactief naar meer proactief.[10] Dit proactieve werk heeft twee verschijningsvormen: verstoren en preventief ingrijpen. Verstoren richt zich op het bemoeilijken van de uitvoering van criminele processen (focus op het heden) en preventief ingrijpen richt zich op het voorkomen van specifieke gebeurtenissen (focus op de toekomst).[11]

De beschikbaarheid van grote hoeveelheden data uit diverse bronnen in combinatie met technologieën om deze data te verwerken, leidt tot een beter inzicht in hoe criminelen te werk gaan bij het plegen van delicten.[12] Dit inzicht kan worden gebruikt om de uitvoering van criminele processen te bemoeilijken. Op dit moment vinden dergelijke verstorende interventies in toenemende mate plaats, in het bijzonder in het kader van de aanpak van digitale criminaliteit.

De ontwikkeling naar meer verstorende interventies heeft echter een breder karakter dan de aanpak van digitale criminaliteit in het algemeen en cybercriminaliteit in het bijzonder. Ook in de aanpak van de 'klassieke' georganiseerde criminaliteit is sprake

6 Landman, Kouwenhoven & Brussen 2020.
7 Sinds 1 maart 2019 mag de politie apparaten hacken die in gebruik zijn bij een verdachte. De Inspectie Justitie & Veiligheid houdt toezicht op de toepassing van de hackbevoegdheid. Zie de rapporten van de Inspectie over de wijze waarop de politie deze bevoegdheid toepast en het rapport van de Hoge Raad (2022).
8 Dit is ook zichtbaar in de komst van data-analisten binnen de recherche. Zie ook hoofdstuk 23.
9 Zie onder andere Landman 2015 voor het straatwerk; Landman, Kouwenhoven & Brussen 2020 voor de recherche; Terpstra 2019 voor de wijkagenten.
10 Zie ook Den Hengst & Wijsman 2023.
11 Zie ook Kirby & Snow 2016.
12 Het gaat nadrukkelijk om 'beter dan voorheen', want het hier bedoelde inzicht in de criminele wereld bestaat uit vele 'blinde vlekken'.

van een steeds beter inzicht in criminele processen en structuren, in het bijzonder voor wat betreft de drugscriminaliteit. De cryptocommunicatiedata hebben hier een belangrijke rol in gespeeld en belangrijker: die moeten hier nog een verdere impuls aan gaan geven, bijvoorbeeld voor wat betreft de omgang met criminele geldstromen.[13] Dit groeiende inzicht wordt in toenemende mate gebruikt voor een meer probleemgerichte aanpak van georganiseerde criminaliteit waarvan het verstoren van criminele processen een onderdeel is. Deze ontwikkeling staat naar mijn indruk nog in de kinderschoenen,[14] maar is wel gaande. Om de probleemgerichte aanpak van georganiseerde criminaliteit te versterken, is de combinatie van technologische en sociale innovatie cruciaal, omdat meer creativiteit in de aanpak gewenst is.

Ook preventief ingrijpen krijgt door een impuls door de beschikbaarheid van grote hoeveelheden data én technologieën om deze data te verwerken. De politie 'produceert' in toenemende mate realtime en toekomstgeoriënteerde intelligence.[15] Deze kennis over wat er gaande is dan wel staat te gebeuren, kan door de politie worden gebruikt als basis voor preventief ingrijpen.[16] Hiermee bedoel ik: ingrijpen voordat het onheil is geschied. De politie komt hiermee niet zozeer 'aan de voorkant' van problemen, maar aan de voorkant van gebeurtenissen. Men probeert om criminaliteit en andere onveiligheidsincidenten *voor te zijn*.[17] Het is een voorzorg- of anticipatielogica.[18] Het doel is niet zozeer om (dieper)liggende oorzaken voor criminaliteit of situationele omstandigheden van criminaliteit duurzaam te beïnvloeden, maar om incidenten te voorkomen. In de Angelsaksische literatuur wordt hiervoor het begrip pre-emptive policing gebruikt (zie ook hoofdstuk 19).

> *'Pre-emptive policing is specifically geared to gather knowledge about what will happen in the future with the goal to intervene before it is too late.'*[19]

13 Zo kunnen de cryptocommunicatiedata worden benut om het criminele (drugs)systeem beter te doorgronden en te komen tot een meer probleemgerichte (systeem)aanpak (zie Tops, 2022). Deze wijze van benutting is nu volop gaande (zie hoofdstuk 12).
14 Zie ook Nelen et al. 2023.
15 Egbert & Leese 2021.
16 Intelligence krijgt hierdoor een meer operationeel karakter en raakt meer verweven met bewijs (zie ook McCulloch & Wilson, 2015).
17 In de Angelsaksische literatuur wordt in dit kader de term *pre-crime* gebruikt (McCulloch & Wilson, 2015; Zedner, 2007). Deze term komt uit *The minority report*, een sciencefictionverhaal van Philip K. Dick uit 1956. In dit verhaal heeft de politie een pre crime eenheid die moorden stopt voordat ze plaatsvinden.
18 Milivojevic 2021; zie ook Gundhus, Skjevrak & Wathne 2023.
19 Van Brakel 2021: 194.

De hier bedoelde vorm van preventief ingrijpen komt nu nog niet op grote schaal voor, maar de praktijken zijn al wel op kleine schaal waar te nemen.[20] Ik noem enkele voorbeelden:

- Risicocommunicatie naar burgers op basis van plaatsgebonden voorspellingen van criminaliteit (bijvoorbeeld over woninginbraken).[21]
- Voeren van stopgesprekken met jongeren die – op basis van geïdentificeerde sociale media berichten – van plan lijken om te gaan rellen.[22]
- Proactief controleren van inzittenden van voertuigen waarvan – op basis van een (algoritmische) risicotaxatie – wordt vermoed dat die zich bezighouden met mobiel banditisme (zie hoofdstuk 17).
- Waarschuwen van (criminele) burgers die met excessief geweld worden bedreigd, op basis van een voorspellend model dat gebruikmaakt van cryptocommunicatiedata (zie hoofdstuk 12).

Dit zijn allemaal voorbeelden van preventief ingrijpen waarbij, op basis van intelligence,[23] wordt geprobeerd om incidenten *voor te zijn*. De voorbeelden laten tevens zien dat er sprake is van diversiteit in de wijze waarop preventief kan worden ingegrepen. Het kan gaan om beschermen, begrenzen en bekrachtigen. *Enforcement* en *support*.[24] Preventief ingrijpen past in het veiligheidsregime van risicobeheersing dat in de afgelopen jaren in uiteenlopende landen aan terrein heeft gewonnen.[25] Dit veiligheidsregime krijgt door big data en AI een stevige impuls, omdat er op grotere schaal risicotaxaties – in wat voor vorm dan ook – kunnen worden uitgevoerd. Het politiewerk aan de horizon zal zich hierdoor bewegen naar meer preventief ingrijpen.

Minder lokaal ingebed politiewerk

Het politiewerk heeft van oorsprong een lokale inbedding. Hiermee bedoel ik dat de keuzes in het politiewerk lokaal worden bepaald en het politiewerk primair in de lokale context wordt uitgevoerd: met verdachten, slachtoffers, samenwerkingspartners en andere actoren die zich in hetzelfde werkgebied van een wijk of een gemeente bevinden. Als gevolg van digitalisering verliest deze lokale inbedding aan betekenis. Dit wil (zeker) niet zeggen dat de lokale inbedding verdwijnt, maar het impliceert wel dat er

20 Zie ook Egbert & Krasmann 2020.
21 Zie ook Egbert & Leese 2021.
22 https://www.politie.nl/nieuws/2021/januari/29/08-politie-zit-bovenop-opruiiers-en-onruststokers.html (voor het laatst geraadpleegd op 23 juli 2021)
23 Hierbij moet worden opgemerkt dat het soms ook gaat om bewijs. Dit heeft te maken met een andere internationale trend die verband houdt met de voorzorglogica: er worden steeds meer voorbereidingshandelingen strafbaar gesteld (zie Lomell, 2018). De grenzen van het strafrecht worden opgerekt: voorheen ging het uitsluitend om de daad of poging daartoe, terwijl tegenwoordig de intentie en motivatie soms ook strafbaar zijn gesteld (zie Schuilenburg, 2016). De bestrijding van terrorisme heeft hierin een katalyserende werking gehad (zie o.a. Hirsch Ballin, 2012; McCulloch & Wilson, 2015; Van Brakel & De Hert, 2011).
24 Zie ook Marciniak 2021.
25 Devroe 2017; Gundhus, Skjevrak & Wathne 2023.

op onderdelen een proces van lokale 'ontbedding' plaatsvindt.[26] Deze ontbedding heeft verschillende typen oorzaken. In het kader van dit boek beperk ik me tot de rol die digitalisering in de lokale 'ontbedding' van politiewerk speelt.

De lokale 'ontbedding' van politiewerk wordt in de eerste plaats beïnvloed door digitalisering van de communicatie tussen burgers. In verschillende hoofdstukken in dit boek is aandacht besteed aan de steeds grotere rol die het internet en in het bijzonder sociale media zijn gaan spelen in de samenleving. Het leven van veel burgers speelt zich af in een werkelijkheid waarin offline en online voortdurend in elkaar overlopen. Gedrag van burgers vindt dus offline en online plaats en dit geldt ook voor gedrag dat voor de politie relevant is. Dit gedrag valt zeker niet allemaal onder de noemer van digitale criminaliteit (zie de volgende alinea). Het gaat ook om online haat, online bedreigingen, online opruiing, online vigilantisme en dergelijke. Deze gedragingen van burgers ten opzichte van elkaar worden niet begrensd door fysieke barrières. Fysieke beperkingen doen zich ook niet voor bij online gemeenschappen die bestaan uit gelijkgestemden die desinformatie verspreiden en voorstellen tot (soms ordeverstorende of ronduit gewelddadige) actie bespreken.[27] De politie in Nederland is bezig met diens aanpassing aan deze 'nieuwe' werkelijkheid. Dit komt onder andere tot uiting in een groeiende praktijk van online surveillance (zie hoofdstuk 16). Online surveillance heeft in beperkte mate een lokale inbedding. Besloten online groepen kunnen hierbij als voorbeeld dienen. Deze groepen houden zich niet aan de grenzen van politiële werkgebieden. Dit wil zeggen dat politiemensen die vanuit een bepaald geografisch gebied in dergelijke groepen aanwezig zijn geregeld burgers uit allerlei andere geografische gebieden tegenkomen (voor zover men dit kan vaststellen).[28] En dat niet alleen: vanwege het grenzeloze karakter van het internet is het goed mogelijk dat politiemensen uit verschillende eenheden aanwezig zijn in dezelfde besloten groep zonder dat zij dit van elkaar weten. Op lokaal of eenheidsniveau keuzes maken met betrekking tot surveillance werkt in die gevallen niet meer. Dit komt door het proces van lokale 'ontbedding'. Om die reden is er op dit moment sprake van een groeiende behoefte aan landelijke (informatie)coördinatie.[29]

De lokale 'ontbedding' van politiewerk wordt daarnaast beïnvloed door de digitalisering van criminaliteit. Digitale criminaliteit heeft tot op zekere hoogte een de-territoriaal of grenzeloos karakter (zie hoofdstuk 6). Dit komt onder andere tot uiting in het gegeven dat dader en slachtoffer(s) van digitale criminaliteit zich vrijwel nooit in dezelfde geografische omgeving van bijvoorbeeld een basisteam van de politie bevin-

26 Ik verwijs hiermee naar het begrip 'disembedding' van socioloog Anthony Giddens. 'By disembedding I mean the "lifting out" of social relations from local contexts of interaction and their restructuring across indefinite spans of time-space.' (Giddens, 1990: 21). Zie ook Terpstra, Fyfe & Salet (2019) over de abstracte politie waarin ook gebruik wordt gemaakt van dit concept.
27 Zie ook NCTV 2022b.
28 Zie Landman & Groothuis 2022.
29 Idem.

den.[30] Bij veel gedigitaliseerde criminaliteit – zoals online oplichting – bevinden dader en slachtoffer zich nog in Nederland, maar voor (hightech) cybercriminaliteit geldt dat de fysieke afstand tussen dader en slachtoffer geregeld over landsgrenzen heen gaat. Dit is een wezenlijk verschil met veel traditionele (veelvoorkomende) criminaliteit waarbij dader en slachtoffer (enigszins) in de buurt van elkaar leven. Naarmate digitale criminaliteit een groter onderdeel wordt van de gehele criminaliteit wordt dit patroon steeds dominanter. Dit creëert een noodzaak om het politiewerk op landelijk en soms op internationaal niveau te coördineren. Dit is in de huidige aanpak van digitale criminaliteit ook zichtbaar. In het kader van de aanpak van gedigitaliseerde criminaliteit is een nieuwe operatie – genaamd Centurion – opgetuigd.[31] Projectvoorstellen voor opsporing worden via een landelijke overlegstructuur over de politie-eenheden verdeeld waar de uitvoering plaatsvindt. De plaats van verdachten is hierbij leidend en niet de plaats waar aangiften zijn binnengekomen.[32] Een dergelijke structuur van landelijke operationele coördinatie is er bij de aanpak van cybercriminaliteit al langer in de vorm van het Landelijk Operationeel Cybercrime Overleg (LOCO). Projectmatige opsporingsonderzoeken – dit zijn in de regel fenomeenonderzoeken – worden daar gewogen en verdeeld tussen de cybercrime teams van de eenheden.[33]

De lokale 'ontbedding' van het politiewerk leidt tot een groeiende behoefte aan – en praktijk van landelijke operationele coördinatie, zo laten de voorbeelden zien.[34] Dit kan op gespannen voet staan met het lokale gezag over de politie.[35] Een situatie waarin basisteams en cybercrimeteams opsporingsonderzoeken landelijk krijgen toegewezen, verhoudt zich bijvoorbeeld niet goed tot het uitgangspunt dat keuzes lokaal of regionaal worden gemaakt. Een regionale stuurploeg kan zich bijvoorbeeld soms afvragen welke invloed men nog heeft op wat er door een cybercrimeteam aan opsporingsonderzoeken wordt opgepakt.[36] Kortom: het lokale gezag paste bij een lokaal ingebedde politie, maar wat zijn de consequenties van de lokale 'ontbedding' van de politie voor het gezag over de politie? Een heroriëntatie op de invulling van het gezag lijkt nodig.[37]

30 Van der Plas, Kuijlaars & Geveke 2022; WRR 2021b.
31 Hierbij baseer ik me op vacatureteksten.
32 Zie ook Kort & Spithoven 2021.
33 Van den Eeden et al. 2021.
34 Ik ben in deze paragraaf niet ingegaan op het vraagstuk van de georganiseerde criminaliteit die – mede met behulp van digitale middelen – op internationale schaal opereert. Het moge duidelijk zijn dat ook dit veiligheidsvraagstuk vraagt om in ieder geval landelijke operationele coördinatie. Hier is nu nog beperkt sprake van, behalve bij de aanpak van specifieke criminele structuren, zoals plaatsvindt in het kader van de Taskforce Aanpak Criminele Machtsstructuren (ACM).
35 Zie ook Van der Plas, Kuijlaars & Geveke 2022.
36 Zie ook Boekhoorn 2019.
37 Van der Plas, Kuijlaars & Geveke 2022.

Minder discretionair politiewerk

De politieorganisatie wordt van oudsher beschouwd als een *street-level bureaucratie* waarin uitvoerende medewerkers relatief autonoom beslissingen kunnen nemen.[38] Deze discretionaire ruimte is een klassiek thema in de politiewetenschap. Mijn verwachting is dat datagedreven politiewerk de discretionaire ruimte van uitvoerende medewerkers reduceert.[39] Er zijn naar mijn idee verschillende factoren die de (verwachte) reductie van de discretionaire ruimte veroorzaken.

De eerste factor is het gebruik van algoritmen in besluitvormingsprocessen. Dit wordt ook wel algoritmische besluitvorming genoemd.

> *'Algoritmische besluitvorming omvat alle processen waarin een algoritme wordt ingezet om beslissingen te nemen die raken aan de rechtspositie van rechtssubjecten of die hen anderszins in hun belangen treffen. Het kan daarbij gaan om gevallen waarin een algoritme zelf een besluit neemt, of gevallen waarin de uitvoer van een algoritme wordt meegenomen in een menselijk besluitvormingsproces.'*[40]

In zowel binnen- als buitenland wordt erop gewezen dat algoritmische besluitvorming in het politiewerk leidt tot een afname van de discretionaire ruimte van uitvoerende politiemensen.[41] De keuzevrijheid van uitvoerende politiemensen wordt door het gebruik van algoritmen beperkt: er zijn in het politiewerk minder keuzes om zelf te maken, bijvoorbeeld doordat een algoritme een situatie als verdacht heeft aangemerkt.[42] Algoritmische besluitvorming heeft – ook in de variant van menselijke besluitvormingsprocessen waarin uitkomsten van algoritmen worden meegenomen – als gevolg dat de rol van (informatie)technologie in het politiewerk verandert: van ondersteunend naar meer beslissend of disciplinerend (zie ook hoofdstuk 20). Dit wil zeggen dat de invloed op de beslissingen die in het politiewerk worden genomen, toeneemt: '…the code enabling programs and algorithms partly shapes the concrete choices of police officers in action.'[43] Deze veranderende rol van technologie in street-level bureaucratieën is een van de redenen waarom men in de bestuurskundige literatuur een nieuw concept heeft geïntroduceerd, te weten: een *system-level bureaucratie*.

38 Lipsky 2010.
39 Zie ook Landman 2022.
40 Kulk & van Deursen 2020: 3.
41 Van Brakel 2021; Brayne 2021; Ferguson 2017a; McDaniel & Pease 2021b; Peeters & Schuilenburg 2018; Ratcliffe, Taylor & Fisher 2020; Terpstra & Salet 2020.
42 In deze paragraaf ligt de nadruk op het algemene patroon. Hierbij moet worden beseft dat de beperking van de keuzevrijheid – en de nog te behandelen verplaatsing van invloed – afhankelijk is van verschillende sociaal-technologische factoren die per type toepassing kunnen verschillen. Algoritmen zijn op verschillende wijzen ingebed in het politiewerk en de uitkomsten beïnvloeden het optreden op uiteenlopende manieren. Zie ook De Kool, Vermeeren & Steijn 2023; Wessels 2023.
43 Niculescu-Dincă 2016: 112.

'In these system level bureaucracies, the discretionary powers of the street-level professionals have been disciplined by digital systems, and the locus of administrative discretion has shifted to those responsible for programming the decision-making process and translating the legislation into software.'[44]

De politieorganisatie is – mede gegeven het niet-autonome karakter van de algoritmische besluitvorming – zeker geen volwaardige system-level bureaucratie.[45] Zij heeft in de afgelopen jaren echter wel meer kenmerken van een dergelijke bureaucratie gekregen en deze ontwikkeling zal zich naar alle waarschijnlijkheid verder doorzetten.[46] Bovenstaande toelichting op de system-level bureaucratie maakt duidelijk dat we niet alleen moeten kijken naar waar de invloed op het politiewerk afneemt, maar ook naar waar de invloed toeneemt. De toenemende invloed treffen we aan bij de eerder behandelde functies die cruciaal zijn voor datagedreven politiewerk (zie hoofdstuk 23). Het gaat dan in het bijzonder – maar zeker niet alleen[47] – om datawetenschappers die algoritmen ontwikkelen en in dat kader allerlei keuzes maken die van invloed zijn op het functioneren van het algoritme.[48] Dit geldt ook voor zelflerende algoritmen: onder andere de trainingsdata die worden geselecteerd en de feedbackdata die worden gebruikt, zijn van invloed op hoe het algoritme zich ontwikkelt (zie ook hoofdstuk 28).[49]

Naarmate de invloed van beslissingsondersteunende systemen op de beslissingen in de uitvoering van het politiewerk toeneemt, neemt de facto ook de invloed van de ontwerpers van deze systemen op het politiewerk toe. *Software engineers worden social engineers*.[50] Naast datawetenschappers en andere specialisten in dienst van de politie gaat het dan ook om bedrijven die slimme softwareprogramma's ontwikkelen.[51] In Nederland lijkt dit – in vergelijking met bijvoorbeeld de VS – beperkt aan de orde te zijn, omdat de politie en bijvoorbeeld het NFI veel systemen zelf ontwikkelen. Dit neemt niet weg dat het zich wel voordoet. Voorbeelden zijn systemen voor online gegevensvergaring, software van het bedrijf Palantir en de hacksoftware die door het Digital Intrusion Team (DIGIT) van de landelijke eenheid wordt gebruikt (zie hoofdstuk 29). Bedrijven hebben via hun systemen (enige) invloed op keuzes die in het politiewerk worden gemaakt. Zo neemt de 'staatsmacht' van bedrijven toe.[52]

44 Zouridis et al. 2019: 313.
45 Een voorbeeld van een volwaardige system-level bureaucratie is de Dienst Uitvoering Onderwijs (DUO) waar beslissingen primair door systemen worden genomen (zie Zouridis, van Eck & Bovens, 2019).
46 Zie ook Terpstra & Salet 2018.
47 Zie ook Wessels (2023) die aangeeft dat de verdeling van invloed over verschillende functionarissen kan bijdrage aan gebrekkige verantwoording.
48 Egbert & Leese 2021; Passchier 2021; Peeters & Schuilenburg 2020; Prins 2020. Zie voor een overzicht en verdieping van deze keuzes: McDaniel & Pease (2021b).
49 McDaniel & Pease 2021b.
50 Susskind 2022.
51 Brayne 2021.
52 Februari 2023.

De tweede factor die de discretionaire ruimte van uitvoerende politiemensen reduceert, ligt in het verlengde van de vorige, maar heeft een iets andere nadruk. Het gaat me nu niet zozeer om de systemen zelf, maar om het gebruik van de output die systemen leveren. Kort samengevat: datagedreven politiewerk brengt de intelligencesturing binnen de politie in een nieuwe fase en dit heeft consequenties voor de discretionaire ruimte in de operatie. De aanpak van de georganiseerde criminaliteit kan dit illustreren. In hoofdstuk 18 is beschreven hoe de politie in Nederland werkt aan het in kaart brengen van de criminele wereld. De data uit verschillende systemen worden gecombineerd en geclassificeerd, zodat er een dataset ontstaat die met analysemethoden kan worden benaderd. Dit maakt het mogelijk om een zo actueel mogelijk beeld van de criminele wereld te presenteren met markten, fasen, rollen et cetera. Dit beeld biedt mogelijkheden om subjecten of entiteiten (zoals bedrijven) te selecteren waarmee (in potentie) criminele netwerken kunnen worden verzwakt (zie ook hoofdstuk 26). Met dit beeld kan zowel op als in de opsporing worden gestuurd. Sturen op de opsporing gaat over welke opsporingsonderzoeken moeten worden gestart.

> *'De centrale positie die de informatieorganisatie claimt in de moderne politieorganisatie doet zo beschouwd afbreuk aan de traditionele autonomie van rechercheurs om hun eigen zaken te ontwikkelen.'*[53]

Sturing in de opsporing heeft betrekking op het bijsturen in lopende opsporingsonderzoeken. In een opsporingsonderzoek richt men zich bijvoorbeeld op subject X en men ziet ook af en toe subject Y (via de tap of andere methode) 'langskomen'. Waar voorheen subject Y wellicht terechtkwam in restinformatie zal er in toenemende mate vanuit het actuele beeld van de criminele wereld worden bijgestuurd. In dit voorbeeld: er wordt aangegeven dat men subject Y moet meenemen als hoofdverdachte, omdat dit niet alleen bijdraagt aan het verzwakken van het criminele netwerk, maar ook substantieel bijdraagt aan de intelligencepositie. Dergelijke vormen van sturing reduceren de autonomie van teamleiders en rechercheurs (en overigens ook van zaaksofficieren).

De aanpak van georganiseerde criminaliteit is een voorbeeld van een bredere ontwikkeling. Hoe meer er een realtime beeld ontstaat van wat er gaande is op het gebied van criminaliteit (zie ook hoofdstuk 17), hoe meer dit beeld zal worden gebruikt om de operatie aan te sturen.[54] Dit verkleint de autonomie van degenen die vooral gewend waren om 'naar bevind van zaken' op te treden. Het bevind van zaken van de betreffende situatie wordt namelijk in toenemende mate in een bredere informatie- of intelligencepositie geplaatst die andere aanknopingspunten tot handelen kan bieden. Die handelingsperspectieven zullen aan uitvoerende politiemensen worden meegegeven

53 Klerks & Vink-Teeven 2020: 173.

54 In die zin er als gevolg van de verdere ontwikkeling van informatiegestuurd politiewerk sprake van een *shift in power structure* (Gundhus, Skjevrak & Wathne, 2023): de intelligenceorganisatie wordt binnen de politie machtiger.

en op de uitvoering ervan zal worden gestuurd.[55] Dit heeft als gevolg dat het pallet aan eigen te maken keuzes minder groot wordt. Anders gezegd: de intelligence logica reduceert de autonomie in het domein van de uitvoering.[56] Deze reductie neemt niet weg dat er – naar mijn indruk – in veel vormen van politiewerk nog voldoende kan worden gekozen door uitvoerende politiemensen.[57] Zij treden daadwerkelijk op. Ook in het tijdperk van datagedreven politiewerk blijft hun vakmanschap cruciaal.

55 Zie ook Niculescu-Dincă (2016) die op basis van literatuuronderzoek de metafoor van het script gebruikt: een script geeft de acteur veel richting, maar is niet deterministisch in het kader van hun optreden.
56 Gundhus, Skjevrak & Wathne 2023.
57 Zie ook Gundhus, Skjevrak & Wathne 2023; Wessels 2023.

25 Politievakmanschap

De veranderingen in het politiemodel en het politiewerk hebben ook consequenties voor het (benodigde) vakmanschap van uitvoerende politiemensen. In dit hoofdstuk staan deze veranderingen centraal. Eerst wordt ingegaan op de verhouding tussen politiemens en politiemachine. Daarna komen enkele (benodigde) veranderingen in het politievakmanschap aan de orde. Het hoofdstuk sluit af met een invalshoek die – naar mijn indruk – nog weleens over het hoofd wordt gezien: het gebruik van opkomende technologieën maakt het werk en vakmanschap van politiemensen binnen de organisatie zichtbaarder.

Tussen politiemens en politiemachine

In zowel de algemene literatuur over AI[1] als de politieliteratuur over datagedreven politiewerk[2] bestaat er geregeld een neiging om mens en machine tegenover elkaar te plaatsen.[3] Technologie en mens zijn dan min of meer concurrenten van elkaar. De vraag of technologie de politiemens kan vervangen, staat op de voorgrond. Dit perspectief doet zich – zoals eerder behandeld (zie hoofdstuk 23) – ook in de praktijk voor: uitvoerende politiemensen kunnen technologie ervaren als een bedreiging voor hun professionele identiteit. Dit bemoeilijkt de adoptie van technologie.

In het hoofdstuk over politievermogens heb ik uitgewerkt dat bepaalde vermogens van politiemensen sterk worden beïnvloed door opkomende technologieën, terwijl dit voor andere vermogens in veel mindere mate het geval is. Naar mijn idee is het in algemene zin zeer waarschijnlijk dat politiemensen en hun vakmanschap in het tijdperk van AI een cruciale rol blijven vervullen in de uitvoering van politiewerk. Dit neemt tegelijkertijd niet weg dat de relatie tussen technologie en politiewerk aan het veranderen is: van secundair naar meer primair, van de randen naar de kern. Dit komt – zoals eerder aangegeven (zie hoofdstuk 20 en 21) – doordat technologie menselijke processen van betekenisgeving in toenemende mate versterkt en ook overneemt.

Deze ontwikkeling zorgt voor gevoelens van onbehagen: wordt een deel van de menselijke autonomie in het politiewerk vervangen door autonomie van AI (zie ook hoofdstuk 24)?[4] Wordt AI op termijn een sterk verbeterde versie van de 'professionele intuï-

1 Zie bijvoorbeeld Daugherty & Wilson 2018; Pasquale 2020.
2 Zie bijvoorbeeld Spithoven & Van de Pas 2020.
3 Er is (gelukkig) ook een wetenschapsgebied waarin de samenwerking tussen mens en machine (AI) centraal staat, getiteld human-centered AI (zie bijvoorbeeld Shneiderman, 2022).
4 Testerink, Nieuwenhuizen & Bex 2023.

tie' van politiemensen?[5] Hoe gaat de balans tussen het versterken van politievakmanschap en het overnemen van politievakmanschap zich ontwikkelen?[6] In een rapport van Interpol wordt hierover het volgende geconcludeerd:

> *'… the law enforcement community is, at present, looking at AI and semi-autonomous systems as instruments with a view to empowering law enforcement personnel in the performance of their duties. The potential of more advance systems to fully automate labor however, goes far beyond this, raising significant questions about the very future of law enforcement as a profession that policy makers will have to carefully consider in the years to come.'*[7]

We weten niet hoe de verhouding tussen politiemens en politiemachine zich op de langere termijn gaat ontwikkelen. We weten wel dat AI op dit moment – en in de nabije toekomst – uitsluitend kan worden ingezet voor specifieke, afgebakende taken (zie ook hoofdstuk 5).[8] AI-systemen zullen steeds meer voor dergelijke taken worden ingezet in vrijwel alle domeinen van het politiewerk. Op basis van de ervaringen die al zijn opgedaan, kan worden geconcludeerd dat het overnemen én versterken van politievakmanschap zich tegelijkertijd voordoen.[9]

Op basis van onderzoek naar de huidige praktijk van datagedreven politiewerk kunnen we tevens concluderen dat er eerder sprake is van samenwerking tussen politiemens en politiemachine dan van concurrentie. Geen of, maar én.[10] De kennis die algoritmische systemen produceren, is in de regel aanvullend op die van politiemensen en moet door politiemensen veelal van nadere interpretatie worden voorzien.[11] In deze interactie tussen politiemens en politiemachine ontstaat een vorm van hybride intelligentie. Werkzaamheden worden dan uitgevoerd op een manier die geen van beide alleen kan realiseren.[12] Bijvoorbeeld: software die wordt gebruikt bij het analyseren van data in opsporingsonderzoek legt verbanden tussen data die politiemensen nooit kunnen leggen, behalve wanneer zij hier per toeval op zouden stuiten. Politiemensen vragen – op basis van deze verbanden – verdachten naar verklaringen op een wijze die een politiemachine vermoedelijk nooit kan overnemen.

5 McGuire 2020.
6 Joh 2018b.
7 Interpol/UNICRI 2019: 20.
8 Waardenburg, Huysman & Agterberg 2020.
9 Hierbij moet worden beseft dat het ook gaat om taken die uitsluitend kunnen worden uitgevoerd, omdat de technologie er is (zie ook hoofdstuk 21). Bepaalde vormen van data-analyse – bijvoorbeeld in opsporingsonderzoek – vonden voorheen simpelweg niet plaats, omdat de data er niet waren of omdat de analyse te arbeidsintensief was om uit te voeren. Van het overnemen van werk kan dan ook geen sprake zijn.
10 De Kool, Vermeeren & Steijn 2023; Marciniak 2021.
11 Egbert & Leese 2021; Marcinak 2021; Niculescu-Dincă 2016; Waardenburg 2021; Zie ook Spithoven & Van de Pas 2020.
12 Waardenburg 2021; zie in meer algemene zin Mols 2023; Pasquale 2020.

Het bovenstaande impliceert dat politievakmanschap – in de praktijk gebracht door politiemensen – cruciaal blijft in het politiewerk aan de horizon. Het politievakmanschap dat voor het politiewerk aan de horizon wordt gevraagd, is op onderdelen wel anders dan het huidige vakmanschap. Dit is ook zichtbaar in tal van andere organisaties die de potentie van opkomende technologieën benutten.[13] Radioloog Curtis Langlotz van *Stanford University* formuleerde het als volgt: 'AI vervangt geen radiologen, maar radiologen die AI gebruiken vervangen radiologen die dat niet doen.'[14] Deze invalshoek lijkt mij ook voor (een deel van de) politiemensen relevant.

Digitaal politievakmanschap

Zoals eerder aangegeven: organisaties die datagedreven willen werken, moeten in zekere zin ook technologiebedrijven worden. Dit geldt ook voor de politie. Dit uitgangspunt vertaalt zich door naar het vakmanschap van medewerkers: alle medewerkers moeten tot op zekere hoogte digitaal bekwaam of breder 'digitaal fit' zijn.[15] Het gevraagde digitaal politievakmanschap omvat diverse aspecten, die ik hier niet allemaal kan benoemen en uitwerken.[16] Ik beperk me tot vijf aspecten waarbij ik per aspect de huidige situatie op hoofdlijnen behandel en daarmee allerlei nuances achterwege laat.

Het eerste aspect is een digitale *mindset*. Onderzoek in het (internationale) bedrijfsleven wijst uit dat digitaal bekwaam begint met een digitale mindset. Een digitale mindset '… is the set of approaches we use to make sense of, and make use of, data and technology. This set of attitudes and behaviors enable people and organizations to see new possibilities and chart a path for the future.'[17] Bij een digitale mindset gaat het om hoe je als medewerker naar het gebruik van technologie in jouw werk kijkt. Een digitale mindset wil zeggen dat je technologie niet ziet als een bedreiging voor jouw werk en jouw identiteit als professional, maar als een kans om het eigen werk verder te verbeteren en te vernieuwen. Een digitale mindset uit zich onder andere in de bereidheid om te investeren in kennis om zodoende de werking van opkomende technologieën op een basisniveau te begrijpen en hierin bij te blijven.[18] Binnen de politie is een digitale mindset vooralsnog niet vanzelfsprekend. In algemene zin geldt dat het kennisniveau van uitvoerende politiemensen met betrekking tot digitale aspecten in het politiewerk laag is.[19] Daarnaast ervaart een deel van hen – zoals eerder aangegeven (zie hoofdstuk 23) – opkomende technologieën als een bedreiging voor de eigen professionele

13 Borek & Prill 2020; Daugherty & Wilson 2018, 2022; Iansiti & Lakhani 2020.
14 Mols 2023.
15 Digitaal fit is een begrip dat is ontwikkeld door Aslander, Broere & Meinema (2022). Zij maken onderscheid tussen vijf pijlers: 1) digitaal bewustzijn, 2) digitale hygiëne, 3) digitale vaardigheden, 4) persoonlijk kennismanagement en 5) persoonlijke groei met behulp van technologie. De focus in dit hoofdstuk ligt op digitaal bewustzijn en digitale vaardigheden.
16 Zo ga ik niet specifiek in op het gevraagde politievakmanschap voor de aanpak van digitale criminaliteit. Dit is wel belangrijk, maar daar is al het nodige over gepubliceerd (zie bijvoorbeeld Jansen et al. 2020). Ik richt me in dit hoofdstuk vooral op technologiegebruik door politiemensen.
17 Leonardi & Neeley 2022.
18 Zie ook Ganesan 2022.
19 Jansen et al. 2020.

identiteit. Hierdoor worden kansen om het eigen werk door middel van technologie te verbeteren niet zomaar gezien en benut.

Het tweede aspect heeft betrekking op datavaardigheden (zie ook hoofdstuk 24).[20] Van uitvoerende politiemedewerkers wordt in toenemende mate gevraagd om het werken met data te integreren in de eigen werkzaamheden.[21] Het werken met data bestaat uit verschillende onderdelen. Allereerst: uitvoerende politiemensen zijn een belangrijke bron van data. Zij creëren in hun werk data. Data liggen in het politiewerk niet klaar om opgeraapt te worden, maar worden in het werk geproduceerd.[22] De keuzes die uitvoerende politiemensen maken ten aanzien van wat zij op welke wijze vastleggen, zijn van belang voor datagedreven politiewerk. De kwaliteit van die data is essentieel. Ik herhaal Elizabeth Joh: *feeding the machine* is een belangrijke opgave.[23] Uitvoerende politiemensen moeten zich ontwikkelen tot 'reflectieve dataprofessionals' die begrijpen hoe het eigen werk leidt tot data en hoe die data worden gebruikt in het kader van datagedreven politiewerk, bijvoorbeeld: de rechercheur die begrijpt hoe data uit opsporingsonderzoeken via classificering worden gebruikt bij veiligheidsanalyse (zie hoofdstuk 18).[24] Uitvoerende politiemensen moeten data daarnaast kunnen interpreteren.[25] Bijvoorbeeld: data die zijn opgeslagen op digitale gegevensdragers zijn een (digitale) weergave of afgeleide van het gedrag van de betreffende burgers, maar het vraagt kennis en vaardigheden om dit gedrag op de juiste wijze te interpreteren.[26] Het belang van deze kennis en vaardigheden is groot, omdat er in het politiewerk met digitale data een (nieuwe) representatie van de werkelijkheid wordt opgebouwd.[27] Data 'spreken niet voor zich'. Het is van belang dat uitvoerende politiemensen ook oog hebben voor wat data allemaal niet vertellen en (dus) buiten de data blijven kijken.[28] Op dit moment zijn uitvoerende politiemensen veelal nog niet de 'reflectieve dataprofessionals' waar datagedreven politiewerk om vraagt. Het vastleggen en interpreteren van data wordt door velen gezien als iets dat naast het echte politiewerk bestaat.[29] Als datagedreven politiewerk een nieuw operationeel model van de politie in Nederland wordt, moet dit veranderen.

> *'Als we serieus en verantwoord met data aan de slag willen gaan, kan dat alleen als we organisatiebreed aan onze interpretatievaardigheden werken.'*[30]

20 In de algemene literatuur over datagedreven werken wordt de term 'datageletterdheid' veel gebruikt (zie bijvoorbeeld Jones, 2020). Dit begrip wordt op uiteenlopende manieren gedefinieerd. Het kunnen interpreteren, beoordelen en ethisch gebruiken van data is in de definities een rode draad (zie Seymoens et al., 2020).
21 De Kool, Vermeeren & Steijn 2023; Roest 2023.
22 Het is van belang te benadrukken dat 'ruwe data' in dat opzicht niet bestaan. Deze term is een oxymoron (zie Rasch, 2020). Er is bij registratie in basissystemen sprake van dataconstructie (Waardenburg, 2021; die ook Landman, 2015).
23 Joh 2017.
24 Waardenburg 2021.
25 Roest 2023.
26 Zie ook Wilson-Kovacs 2021.
27 Veldhuizen 2023.
28 Idem.
29 Zie bijvoorbeeld Landman, Kouwenhoven & Brussen 2020.
30 Veldhuizen 2023: 171.

Een derde aspect gaat over het gebruik van slimme software.[31] Uitvoerende politiemensen worden in toenemende mate – en wat futuristisch geformuleerd – operators van politiemachines en moeten kunnen omgaan met algoritmen. De mate waarin dit het geval is of zal zijn, verschilt tussen werkterreinen binnen de politie. In het straatwerk zal de mens-machine-interactie een minder intensief karakter hebben dan in het (data-intensieve) intelligencewerk en opsporingswerk. Het werken met analysetools om grote hoeveelheden data te analyseren is echter nog lang geen gemeengoed binnen de politieorganisatie.[32] Het wordt vooral gezien als werk van onder andere analisten en data specialisten, maar op termijn zal dit een meer generiek onderdeel van het politiewerk en daarmee van het politievakmanschap moeten worden.[33] Hierbij doet zich een lastig patroon voor: hoe meer het werk wordt belegd bij specialisten, des te meer de generalisten het werk doorschuiven naar specialisten en hoe meer generalisten dit doen, des te meer het werk moet worden belegd bij specialisten (want generalisten ontwikkelen de benodigde vaardigheden niet). Het gevraagde vakmanschap heeft niet alleen betrekking op het gebruik van de software, maar ook op het omgaan met de uitkomsten die worden gegenereerd. Dit vraagt enig begrip van hoe software en algoritmen werken.[34] Welke data worden op welke wijze gebruikt en welke conclusies kunnen (niet) aan de uitkomsten worden verbonden?[35] Het is immers – mede vanwege wet- en regelgeving (zie ook hoofdstuk 27) – altijd de politiemens die verdergaat met de uitkomsten van slimme systemen en op basis daarvan tot definitieve besluiten en volgende acties komt. Politiemensen moeten kunnen uitleggen hoe de uitkomsten van slimme systemen hun eigen proces van beeld-, oordeels- en besluitvorming heeft beïnvloed. Naast begrip van de software worden ook analysevaardigheden steeds crucialer. Naarmate de analysesoftware meer wordt gebruikt door generalisten in plaats van specialisten zullen generalisten meer zelf (moeten) gaan analyseren.[36] In een van de politiekorpsen in het VK – waar men experimenteert met slimme software in opsporingsonderzoeken – is *everyone's an analyst* een gevleugelde uitspraak.[37] Deze uitspraak illustreert deze ontwikkeling.[38] Hier

31 Zie in meer algemene zin: Borek & Prill 2020.

32 Den Hengst 2017; Roest 2023; zie ook Dewald 2023.

33 Hiervoor is van belang dat analysetools laagdrempelig en enigszins intuïtief kunnen worden gebruikt, want anders is de stap (te) groot om eraan te beginnen en zodoende de vaardigheden te ontwikkelen (zie ook Roest, 2023)

34 Waardenburg 2021.

35 Marciniak (2021) haalt in zijn proefschrift naar datagedreven politiewerk in het VK een voorbeeld aan van risicotaxatie op persoonsniveau waarbij politiemensen naar aanleiding van de uitkomsten regelmatig de onderliggende data van de betreffende personen bestuderen om zodoende de uitkomsten te kunnen begrijpen en deels ook te controleren.

36 Klerks & Vink-Teeven 2020.

37 Marciniak 2021.

38 Een dergelijke ontwikkeling is op termijn ook waarschijnlijk in forensisch onderzoek (zie hoofdstuk 11). De ontwikkeling van mobiele identificatietechnologie c.q. DNA-analyse kan er op termijn voor zorgen dat rechercheurs zelf eenvoudig DNA-onderzoek kunnen verrichten. De rol van de forensisch expert wordt in die gevallen meer faciliterend, door bij te dragen aan de ontwikkeling van tools en methoden en toe te zien op de kwaliteit van processen (zie Mapes, 2017). In digitaal onderzoek is een veranderende rolverdeling al langzaam gaande. Zie hiervoor ook hoofdstuk 13, in het bijzonder met betrekking tot TROI.

ligt nog een opgave: het is niet vanzelfsprekend dat uitvoerende politiemensen beschikken over adequate analysevaardigheden.[39]

Een vierde aspect heeft betrekking op de juridische aspecten van datagedreven politiewerk (zie ook hoofdstuk 27). Hoe meer politiemensen 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 (Wpg). Het gaat hierbij om algemene principes – zoals doelbinding, proportionaliteit en dataminimalisatie – en specifieke onderdelen en artikelen die op het eigen werk van toepassing zijn. Hoewel dit niet altijd zo wordt ervaren, is de Wpg voor het politiewerk net zo belangrijk als het Wetboek van Strafvordering.[40] Naast de Wpg is ook andere wet- en regelgeving van belang, waaronder het Wetboek van Strafvordering. Politiemensen 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. Dit hoort bij politievakmanschap. Binnen de politie is de omgang met - en correcte naleving van de Wpg echter 'weerbarstige materie'.[41] Dit aspect van het vakmanschap heeft in het kader van datagedreven werken aandacht nodig.

Een vijfde en laatste aspect gaat over de vaardigheden om bij te dragen aan het ontwikkelen en functioneren van technologie. Dit wordt in de literatuur ook wel 'democratisering van technologie' genoemd. In allerlei organisaties worden uitvoerende medewerkers gevraagd om een bijdrage te leveren aan technologieontwikkeling teneinde zichzelf te kunnen laten versterken door technologie.[42] De inbreng van uitvoerende politiemensen bij het ontwikkelen van slimme systemen is cruciaal, omdat zij domeinkennis hebben[43] en uit praktijkervaringen kunnen putten.[44] Om te kunnen bijdragen, hoeven zij geen expert in AI te zijn, maar (basis)begrip van hoe nieuwe technologie werkt, is wel gewenst.[45] Naast bijdragen aan ontwikkeling is het bijdragen aan het functioneren van slimme systemen van belang. Deze bijdrage krijgt onder andere gestalte door feedback te geven aan systemen, bijvoorbeeld: is er bij een proactieve controle op basis van een melding van een slim systeem inderdaad iets aangetroffen wat

39 Den Hengst 2017; Roest 2023.
40 Den Hengst & Wijsman 2023. Dit impliceert overigens ook dat de rol van de informatieofficier (OM) steeds belangrijker wordt.
41 Tazelaar 2017; zie ook Winter et al. 2020.
42 Daugherty & Wilson 2018.
43 In organisaties die vooroplopen in het gebruik van AI is een nieuwe ontwikkeling gaande waarbij er naast machine learning (leren van data) ook machine teaching plaatsvindt. 'The human turn in intelligent systems is upending many of the assumptions about the role of people and their expertise in the emerging technological ecosystem. This is one of the most consequential human turns of all: from machines "learning" by processing mountains of data to humans teaching machines based on human experience, perception, and intuition (Daugherty & Wilson, 2022: 16). Machine teaching is een combinatie van machinaal leren en machinaal redeneren (zie hoofdstuk 4, zie ook Mols, 2023). Ik denk dat machine teaching onder andere van meerwaarde is voor het ontwikkelen van systemen die suggesties kunnen doen voor interventies (zie o.a. hoofdstuk 19).
44 Dit vindt nu al plaats in bijvoorbeeld het Productiehuis, TROI en (andere) innovatieteams (zie hoofdstuk 24) en zal in de komende jaren naar verwachting verder toenemen.
45 Waardenburg 2021: 120.

wijst op (het voorbereiden van) een strafbaar feit? Het geven van feedback aan een systeem is een belangrijke vorm van samenwerking tussen politiemens en politiemachine, omdat systemen niet slim kunnen zijn en blijven zonder de inbreng van politiemensen. Dit punt leidt ons in essentie terug naar datavaardigheden, omdat het geven van feedback ook registratie vereist.

Bovenstaande punten geven gezamenlijk (enige) invulling aan de inhoud van digitaal vakmanschap. Het ontwikkelen van digitaal vakmanschap binnen de politie vraagt om een combinatie van instroom van nieuwe politiemensen met een – op onderdelen – ander profiel dan voorheen én om investeringen in de ontwikkeling van bestaande medewerkers. Het gebruik van technologie door politiemensen – technologie-adoptie (zie hoofdstuk 23) – zal binnen de organisatie meer aandacht moeten krijgen.[46] Leren in de praktijk heeft de voorkeur waarbij degenen die beginnen met het gebruik van bepaalde software hun collega's kunnen 'besmetten'.[47] Het citaat van de radioloog is hierbij naar mijn idee een belangrijk uitgangspunt: het werk van politiemensen wordt door de bank genomen niet overgenomen door AI, maar politiemensen die geen gebruik maken van AI worden op termijn wel vervangen door politiemensen die dit wel doen.[48]

Zichtbaarheid en monitoring van politievakmanschap
Een van de eerste studies in ons land naar het gebruik van informatietechnologie door uitvoerende politiemensen – het gaat dan om de eerste geïntegreerde basisprocessen systemen en experimenten met mobiele data terminals in politieauto's – is het promotieonderzoek van Wouter Stol dat in 1996 is gepubliceerd.[49] In dit onderzoek concludeerde hij dat informatietechnologie niet zozeer leidde tot meer sociale controle van burgers, maar tot meer sociale controle van politieagenten. Anders gezegd: politieagenten werden meer gemonitord en gecontroleerd.

Deze conclusie is ook voor opkomende technologieën van belang.[50] Het gaat dan niet zozeer om het eerste deel van de conclusie – want er is in de sociale controle van burgers met behulp van technologie wel wat veranderd sinds de jaren negentig van de vorige eeuw (zie ook hoofdstuk 27) – maar om de constatering dat informatietechnologie leidt tot sociale controle van uitvoerende politiemensen. Veel van de technologie die in het politiewerk wordt gebruikt, biedt niet alleen de mogelijkheid om burgers

46 Op LinkedIn las ik via Martijn Aslander een quote die naar mijn idee van toepassing is op de huidige situatie: 'IT mensen houden zich bezig met hoe computers werken. HR mensen houden zich bezig moet hoe mensen werken. Niemand houdt zich bezig met hoe mensen met computers werken.'
47 Zie ook Jansen et al. 2020; Roest 2023.
48 Dit is een algemene uitspraak die geen recht doet aan de verschillen tussen taakvelden. Niet iedere taakveld zal in dezelfde mate worden beïnvloed door het gebruik van AI.
49 Stol 1996.
50 Het gaat dan om de toenemende monitoring van politiemensen. Met betrekking tot intensievere sociale controle van burgers is er – naar mijn idee – wel wat veranderd sinds het proefschrift van Wouter Stol. Zie hiervoor onder andere hoofdstuk 27.

beter in beeld te brengen, maar brengt ook de activiteiten van politiemensen beter in beeld.[51] Bodycams zijn hiervan het meest duidelijke voorbeeld, omdat expliciet wordt beoogd dat het corrigerende en controlerende effect twee kanten op werkt: de burger wordt gefilmd, maar de politie ook.[52] Bij andere toepassingen is het zichtbaar maken van de activiteiten van politiemensen niet het primaire doel, maar kan hiervoor wel worden benut. Global Positioning System (GPS)-data kunnen bijvoorbeeld worden gebruikt om te volgen waar politieagenten zijn en te beoordelen of ze wel gaan naar de plaatsen waarnaar zij – al dan niet met behulp van *predictive policing* – zijn 'gestuurd'.[53] Ook de invoer van gegevens door politieagenten kan worden gebruikt om de kwaliteit van het (data)werk te beoordelen.[54] Als gevolg van *function creep* – het gebruik van data voor andere doeleinden dan waarvoor ze waren bedoeld – worden degenen die anderen in de gaten houden (*the watcher*) ook zelf in toenemende mate in de gaten gehouden (*the watched*).

> *'This surveillance gaze represents an uncomfortable inversion of officers' usual surveillance work and is part of the crisscrossing attending function creep: no one, not even the police, is exempt from surveillance today.'*[55]

Door activiteiten zichtbaar te maken en data over uitvoerende politiemensen te verzamelen, kan hun vakmanschap worden gemonitord. In de VS en het VK zijn er politiekorpsen die bijvoorbeeld slimme software gebruiken om inzicht te krijgen in welke politiemensen risico lopen op escalerend gedrag in interacties met burgers.[56] Hierbij wordt gebruikgemaakt van data over het aantal aanhoudingen, geweldgebruik, klachten van burgers en dergelijke. Door middel van algoritmen vindt risicotaxatie plaats. Bij 'risicovolle' medewerkers komen vlaggetjes te staan of leidinggeven krijgen geautomatiseerd een mail als een medewerker in een bepaalde risicocategorie terechtkomt. Leidinggevenden kunnen op basis hiervan actie ondernemen, bijvoorbeeld in de vorm van een gesprek.[57] Kortom: in het tijdperk van 'big data' worden ook politiemensen object van risicotaxatie.

Ook in Nederland zijn de afgelopen jaren programma's ontwikkeld waarmee politiemensen worden gemonitord. Een (bekend) voorbeeld is het algoritme dat 'opvallend zoekgedrag binnen politiesystemen in een vroegtijdig stadium moet detecteren' om zodoende het lekken van vertrouwelijke informatie tegen te gaan.[58] Het programma 'scoort' politiemensen op basis van hun zoekgedrag in de politiesystemen. Een leiding-

51 Waardenburg, Huysman & Agterberg 2020.
52 Flight 2017.
53 Ariel 2019; Brayne 2021; Ericson & Haggerty 1997; Ferguson 2017a; Niculescu-Dincă 2016.
54 Marciniak 2021.
55 Brayne 2021: 82.
56 Ferguson 2017a; Marciniak 2021.
57 Ferguson 2017a.
58 https://www.nrc.nl/nieuws/2020/12/06/politie-gaat-lekken-bestrijden-met-computerprogramma (voor het laatst geraadpleegd op 21 oktober 2022).

gevende beoordeelt deze score vervolgens alvorens er eventuele opvolging aan signalen wordt gegeven, door bijvoorbeeld een gesprek. Mocht er sprake zijn van vermoedelijk plichtsverzuim of crimineel lekken, dan volgt het gebruikelijke disciplinaire onderzoek, aldus de projectleider van het betreffende project. Dit programma illustreert dat technologie (in toenemende mate) ook als een oplossing voor interne problemen wordt beschouwd.[59]

Met deze uiteenzetting over toegenomen zichtbaarheid en monitoring van vakmanschap van uitvoerende politiemensen is dit hoofdstuk en dit deel afgesloten. We zijn nu aanbeland bij het laatste deel van dit boek. Dit gaat over de gevolgen van opkomende technologieën in het politiewerk voor publieke waarden. Kortom: het perspectief van de samenleving staat centraal.

59 Brayne 2021.

Deel V Publieke waarden

26 Effectiviteit

De 'million-dollar question' is natuurlijk hoe effectief datagedreven politiewerk is.[1] In dit hoofdstuk ga ik in op deze vraag. Om maar 'met de deur in huis te vallen': deze vraag kan (nog) niet worden beantwoord. In paragraaf 1 geef ik hier de redenen voor. In de paragrafen die volgen, ga ik in op de mogelijk bijdrage van datagedreven werken aan verschillende vormen van effectiviteit van politiewerk – voorkomen, detecteren, tegenhouden en ophelderen van criminaliteit – en de werkingsmechanismen die hierbij een rol spelen. Het hoofdstuk sluit af met een conclusie.

Waarom we vooralsnog weinig weten

Hoewel de verwachtingen van de opbrengsten van het gebruik van opkomende technologieën in het politiewerk vaak hoog zijn,[2] zijn uitspraken over de bijdrage aan de effectiviteit van politiewerk op dit moment – zoals gezegd – lastig te doen. Dit heeft verschillende redenen.

De eerste reden heeft te maken met de effectiviteitsvraag als zodanig. Effectiviteit moet – simpel gezegd – worden opgevat als doelbereiking. Dit roept de vraag op wat de doelen van de politie zijn. Die vraag is niet gemakkelijk te beantwoorden. De politie is in formele zin namelijk een organisatie met een taak en niet met een doel. Die taak is omschreven in artikel 3 van de Politiewet en heeft betrekking op de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven. Anders gezegd: de politie moet iets doen, niet per se iets bereiken. Dit neemt niet weg dat de politie in beleidsmatige zin doelen kan formuleren. Het punt is echter dat hierbij vele doelen als uitgangspunt kunnen worden genomen. Ik noem er een paar:[3] snel ter plaatse zijn, misdrijven ophelderen, crimineel geld afpakken, misdrijven voorkomen, (geregistreerde) criminaliteit reduceren, criminaliteit tegenhouden of beheersbaar houden, problemen van burgers in de wijk oplossen, de vrede bewaren, onveiligheidsgevoelens onder burgers verminderen en vertrouwen van burgers in de politie vergroten. Naarmate de doelen minder direct verband houden met de taken van de politie, heeft de politie in de regel minder invloed op de doelbereiking. Bijvoorbeeld: het ophelderingspercentage is, met alle mitsen en maren, een maatstaf voor effectiviteit waar de politie meer invloed op heeft dan op de omvang van de geregistreerde criminaliteit.

1 Ferguson 2017a.
2 Terpstra & Salet 2020.
3 Zie ook Van Reenen 2012.

Doelen die minder direct verband houden met de taken, vragen vaker om een samenspel tussen verschillende partijen.[4] Naast deze punten – die in essentie gaan over wat zinvolle indicatoren voor effectiviteit van politiewerk zijn – moet tevens worden geconstateerd dat het meten van effectiviteit in methodische zin een ingewikkelde opgave is.[5] Kortom: het beantwoorden van de vraag naar effectiviteit van politiewerk – of het nu datagedreven is of niet – is problematisch of op zijn minst uitdagend.[6]

Dan nu naar de vaag naar effectiviteit van datagedreven politiewerk. Wat maakt het lastig om uitspraken over de effectiviteit van dit politiemodel te doen? Het is ten eerste vroeg om de effectiviteitsvraag te stellen. Het gebruik van opkomende technologieën – in het bijzonder AI – in het politiewerk bevindt zich in een beginstadium.[7] Dit is ook zichtbaar in deel III van dit boek: het gaat vaker om experimenten dan om toepassingen die breed geïmplementeerd zijn en al jaren worden gebruikt. De effectiviteit van datagedreven politiewerk is vooral een verwachte of aangenomen effectiviteit. De aanname met betrekking tot de effectiviteit is vooral gebaseerd op de constatering dat opkomende technologieën de vermogens van de politie substantieel (gaan) beïnvloeden op een manier die historisch gezien nieuw is.[8] We weten echter niet of nauwelijks of deze vergrote vermogens ook leiden tot politiewerk dat effectiever is dan voorheen.

Een punt dat met het voorgaande samenhangt en eveneens van invloed is op het (kunnen) doen van uitspraken over de effectiviteit van datagedreven politiewerk heeft betrekking op het onderscheid tussen de directe opbrengsten van technologiegebruik én de interventies die op basis hiervan al dan niet worden uitgevoerd. Anders gezegd: er is een onderscheid tussen de effectiviteit van de technologie zelf en de effectiviteit van het optreden dat mede op basis van de technologie plaatsvindt.[9] Uitspraken over de eerste vorm van effectiviteit zijn vermoedelijk gemakkelijker te doen dan de tweede. Dit heeft niet alleen te maken met het gegeven dat het lastig is om de effectiviteit van politieoptreden vast te stellen, maar ook met de eerder gedane constatering dat technologiegebruik niet per definitie tot een andere manier van werken leidt (zie hoofdstuk 23). Zonder 'juiste' adoptie van technologie valt er van invloed op de effectiviteit van het optreden niet veel te verwachten. Bijvoorbeeld: technologie kan bijdragen aan de kwaliteit van veiligheidsbeelden, maar dit wil niet zeggen dat er probleemgericht mee wordt gestuurd en gewerkt. Het kost op zijn minst tijd om de verandering naar een andere manier van werken te realiseren.[10] Dit is een bijkomende reden dat het vroeg is om iets over de effectiviteit van datagedreven politiewerk te zeggen.

4 Zie ook Terpstra 2010a.
5 Zie ook Van Reenen 2012.
6 Zie ook Ferguson 2017a; Terpstra 2010a.
7 Joh 2018a.
8 Joh 2018b.
9 Terpstra & Salet 2020.
10 Zie ook Koper, Lum & Willis 2014.

Het gegeven dat veel ontwikkelingen zich in een beginstadium bevinden, is een van de oorzaken dat (evaluatie)onderzoek naar datagedreven politiewerk – zowel nationaal als internationaal – schaars is. Het (evaluatie)onderzoek dat in (inter)nationaal verband wel is verricht, is eenzijdig gericht op vormen van predictive policing en dan in het bijzonder op predictive mapping.[11] Onderzoek naar andere vormen van datagedreven politiewerk is niet of nauwelijks verricht.[12] Dit maakt het logischerwijs ook lastig om onderbouwde uitspraken over de effectiviteit van datagedreven politiewerk te doen.

Een vijfde en laatste reden dat uitspraken over de effectiviteit lastig zijn te doen, hangt samen met de vorige reden, maar moet wel apart worden benoemd: de variëteit in datagedreven politiewerk maakt dat het niet mogelijk en zinvol is om in algemene zin iets te zeggen over de effectiviteit. Uitspraken over de effectiviteit van datagedreven politiewerk moeten naar mijn mening worden gespecificeerd voor zowel de toepassing als de dimensie van effectiviteit. Dat is ook waar het nu aan ontbreekt. De uitspraken die in de internationale literatuur worden gedaan over de effectiviteit van *big data policing* zijn vooral gebaseerd op predictive policing, maar big data policing omvat – zoals gezegd – veel meer dan predictive policing. Door uitspraken over de effectiviteit van datagedreven politiewerk te baseren op predictive policing wordt geen recht gedaan aan de variëteit in datagedreven politiewerk. Mijn vermoeden is dat dit in wetenschappelijke publicaties eerder leidt tot een onderschatting dan overschatting van de effectiviteit van datagedreven politiewerk. Anders gesteld: wie onderzoeksresultaten van de pilots met het CAS (zie hoofdstuk 19) betrekt bij de eerste oordelen over de effectiviteit van datagedreven politiewerk komt tot hele andere indicaties van die effectiviteit dan wie kijkt naar de strafrechtelijke opbrengsten van de cryptocommunicatiedata (zie hoofdstuk 12). Het is van belang om dit goed voor ogen te houden bij het doen, maar ook bij het interpreteren van algemene uitspraken over de effectiviteit van datagedreven politiewerk.

Het voorgaande neemt niet weg dat ik de (mogelijke) effectiviteit van datagedreven politiewerk hierna ga verkennen. Dit doe ik door in te gaan op verschillende verschijningsvormen van effectiviteit waarbij ik zo veel mogelijk specificeer welk typen toepassingen een rol spelen.

Voorkomen van criminaliteit

Het voorkomen van criminaliteit verwijst naar het eerder behandelde preventief ingrijpen van de politie (zie hoofdstuk 24): ingrijpen voordat een incident plaatsvindt. Om te kunnen voorkomen, wordt criminaliteit voorspeld of eigenlijk: worden er risico's getaxeerd. Plaatsen en personen worden door algoritmen in een risicocategorie ge-

11 Het evaluatieonderzoek dat naar predictive identification is verricht, heeft vooral betrekking op de accuraatheid van voorspellingen op het gebied van recidive (zie hoofdstuk 19).

12 Zie ook De Kool, Vermeeren & Steijn 2023.

plaatst. Een hoge risicocategorie wil zeggen dat de aandacht en het optreden van de politie zich hier meer op zou moeten richten. Effectiviteit wil in dit kader in de eerste plaats zeggen dat de risicotaxaties accuraat zijn en tot weinig valspositieven of valsnegatieven leiden (zie ook hoofdstuk 28). Bij het beoordelen van de accuraatheid van (zelflerende) algoritmen is het niet 'eerlijk' om perfectie als uitgangspunt te nemen.[13] Slimme, datagedreven (AI)-systemen voor risicotaxatie moeten accurater zijn dan expertsystemen die gebruik maken van modelgedreven algoritmen én dan menselijke inschattingen.[14] Wanneer hier sprake van is, kan worden gesproken van effectiviteit op het niveau van de toepassing. Of hier op dit moment sprake van is, is niet eenduidig aan te geven. De uitkomsten zijn wisselend (zie hoofdstuk 19).[15] Hierbij moet worden opgemerkt dat er, zeker in Nederland, nog niet zoveel AI-toepassingen zijn. Een ander aspect van effectiviteit op het niveau van de toepassing is of het tot nieuwe inzichten leidt (die ook accuraat zijn). Bijvoorbeeld: komt een slim systeem met 'risicovolle personen' die de politie nog niet op het netvlies heeft staan? Eerste ervaringen in het buitenland doen vermoeden dat dit (soms) het geval is (zie hoofdstuk 19).

Als accurate risicotaxaties worden gebruikt voor het optreden, dan kunnen deze leiden tot het voorkomen van delicten en andere gebeurtenissen, zoals openbare orde-verstoringen. Van effectiviteit is sprake als voorbereidingen of eerste handelingen van de daders 'in wording' worden beëindigd en/of wanneer potentiële slachtoffers in staat worden gesteld om maatregelen te nemen. In welke mate dit – als gevolg van risicotaxaties – het geval is, weten we niet. Er is slechts anekdotisch bewijs. Wat we wel weten, is dat de wijze van optreden kan uitmaken. De politie heeft hierin keuzes. Je kunt informatie over een hoog risicogebied meegeven aan een noodhulpauto, maar je kunt er ook een 'vrije' (burger)auto voor inzetten. Het laatste bleek in een experiment in Philadelphia effectiever.[16] Je kunt een persoon die als hoog risico is aangemerkt intensiever controleren, maar ook samen met anderen in beschermende factoren (zoals opleiding, werk, zorg) investeren. Dit zijn slechts voorbeelden; het gaat erom dat de wijze van opvolging vermoedelijk van invloed is op de effectiviteit. Er is weinig reden om aan te nemen dat datagedreven politiewerk effectiever is dan voorheen wanneer de opvolging hetzelfde is als voorheen. Daarom is sociale vernieuwing belangrijk.

Bij het voorkomen van criminaliteit moet worden benadrukt dat de potentie van effectiviteit vooral betrekking heeft op het wegnemen van de directe oorzaken van criminaliteit: iemand is iets van plan of al ergens aan begonnen en maakt het niet af of slaagt er niet in. Datagedreven politiewerk lijkt minder mogelijkheden te bieden om dieperlig-

13 Zie ook Terpstra & Salet 2020.
14 Vestby & Vestby 2019.
15 Dit is een bijkomende reden dat het doen van uitspraken lastig is. Voor zover evaluatieonderzoek is verricht, zijn de uitkomsten wisselend. Dit komt naar mijn idee onder andere doordat men de omvang van (bepaalde) criminaliteit geregeld als afhankelijke variabele in het onderzoek betrekt. Tussen de onafhankelijke variabele 'gebruik van predictive mapping' en de afhankelijke variabele 'omvang van een delict' spelen vermoedelijk een heleboel factoren een rol. Dit kan leiden tot wisselende uitkomsten.
16 Ratcliffe et al. 2021.

gende oorzaken te beïnvloeden (zie ook hoofdstuk 24). Dit heeft niet alleen te maken met het gegeven dat de politie de oorzaken van criminaliteit niet of nauwelijks kan beïnvloeden,[17] maar ook met de aard van de inzichten die datagedreven werken oplevert. Datagedreven risicotaxaties zijn gebaseerd op correlatie: samenhang in de data. Daarmee is er nog geen inzicht in causaliteit: oorzaken.[18] Anders gezegd: risicofactoren zijn nog geen causale factoren.[19] Als een gebied als een hoog risicogebied voor woninginbraken is aangemerkt, weet je niet (precies) *waarom* daar waarschijnlijk meer woninginbraken worden gepleegd dan elders. Dit geldt ook voor het taxeren van risicovolle personen. Causale vragen kunnen nooit – of in ieder geval niet op dit moment – op datagedreven wijze worden beantwoord.[20] Het gegeven dat datagedreven (predictieve) toepassingen geen inzicht geven in causaliteit wil overigens niet zeggen dat er geen aangrijpingspunten voor opvolging in de vorm van preventie zijn.[21] Als je weet dat bepaalde personen waarschijnlijk gaan doorgroeien in de georganiseerde criminaliteit, dan is dat in principe voldoende om tot interventies te komen. Juist hier is de combinatie tussen politiemachine en politiemens van meerwaarde en misschien kan er in de toekomst datagedreven inzicht in de effectiviteit van interventies ontstaan om politiemensen ook daarbij te ondersteunen (zie hiervoor hoofdstuk 19).

Het voorgaande leidt tot de conclusie dat de potentiële bijdrage van datagedreven politiewerk aan het voorkomen van criminaliteit plaatsvindt via 1) accuratere risicotaxaties die tot nog toe onbekende risico's inzichtelijk maken, en 2) manieren van optreden op basis van die risicotaxaties die ervoor zorgen dat de getaxeerde gebeurtenissen en gedragingen niet plaatsvinden.[22] Er zijn voorbeelden waarin er van beide sprake is en er van effectiviteit kan worden gesproken, bijvoorbeeld het waarschuwen van personen die vermoedelijk slachtoffer zouden worden van excessief geweld (zie hoofdstuk 12). Van daadwerkelijke onderbouwing dat datagedreven politiewerk bijdraagt aan het voorkomen van criminaliteit is echter nog geen sprake. Meer onderzoek hiernaar is nodig, maar is complex, want het is buitengewoon lastig om aan te tonen dat iets niet is gebeurd als gevolg van een interventie (dat anders wel gebeurd zou zijn).

Detecteren van criminaliteit

Het detecteren van criminaliteit gaat over het vaststellen van (de uitvoering van) een strafbaar feit op het moment dat het plaatsvindt, zodat de daders vrijwel direct kunnen

17 Zie o.a. Terpstra 2010a.

18 Zie ook Spithoven & Van de Pas 2020.

19 Zie bijvoorbeeld De Vries et al. 2021; Snaphaan et al. 2023.

20 Pearl & Mackenzie 2019.

21 De stelling van Andrew Ferguson (2017a: 47) – 'Data identifies the disease but offers no cure' – is wat mij betreft dan ook wat te gemakkelijk. Ook bij causaal inzicht presenteert de meest effectieve interventie zich niet als vanzelf.

22 Wellicht ten overvloede: dit is nog iets anders dan een meer algemene reductie van de betreffende delicten. Dit is naar mijn idee een minder realistische maatstaf. Een hypothetisch voorbeeld: als de liquidaties in de drugswereld toenemen, wil dit niet zeggen dat de risicotaxaties en interventies van het Threat To Life team niet effectief zijn. Het wil vooral zeggen dat er een maatstaf voor effectiviteit is gekozen die niet direct verband houdt met de technologische toepassing en daarop gebaseerde interventies.

worden aangehouden. Effectiviteit wil in dit kader zeggen dat er verhoudingsgewijs meer strafbare feiten worden vastgesteld terwijl ze plaatsvinden en vooral dat de pakkans van daders wordt vergroot (heterdaadkracht).[23] De potentiële bijdrage van datagedreven politiewerk aan de effectiviteit in termen van het detecteren van criminaliteit vloeit vooral voort uit de uitbreiding van het waarnemingsvermogen van de politie (zie hoofdstuk 21). Door middel van een toenemend aantal sensoren kan er in potentie meer criminaliteit worden gedetecteerd, omdat het bereik van observatie wordt vergroot en sensoren 24/7 waarnemen.[24] Het gaat hierbij niet alleen om afzonderlijke sensoren, maar (zeker) ook om de voorzieningen waarmee data uit verschillende sensoren en andere bronnen worden gecombineerd en van betekenis worden voorzien, bijvoorbeeld in termen van verdachte situaties (zie hoofdstuk 17).[25]

> *'New surveillance technologies have the potential to exponentially increase our ability to detect, investigate and prosecute criminal activity.'*[26]

Datagedreven politiewerk kan dus bijdragen aan heterdaadkracht. Het eerder behandelde voorbeeld van de aanhouding van de (destijds) verdachten van de moord op Peter R. de Vries is een illustratie van heterdaadkracht. Het werkingsmechanisme is eenvoudig: door sensoren wordt iets waargenomen en daar wordt op gereageerd door politiemensen. Dit werkingsmechanisme werkt echter alleen als iets wordt vastgesteld c.q. gesignaleerd en de politie *snel* 'ter plaatse' komt. In het ANPR-voorbeeld van Peter R. de Vries is de signalering eenvoudig – een kenteken die in een database staat, wordt door een camera waargenomen (zie hoofdstuk 14) – maar voor het detecteren van crimineel of verdacht gedrag zijn meer geavanceerde algoritmen nodig. Dit geldt ook voor het inschatten van vluchtroutes van daders (zie hoofdstuk 17). Voor deze algoritmen geldt hetzelfde als voor algoritmen in het kader van predictive policing: accuraatheid is van belang voor effectiviteit. Over de accuraatheid van dergelijke algoritmen weten we – op basis van wetenschappelijk onderzoek – vooralsnog weinig. In de sensing proeftuin in Roermond is volgens de politie (in 2019) een accuraatheid van ongeveer 50% gerealiseerd (zie hoofdstuk 17). Dit wil zeggen dat 50% van de daadwerkelijk gecontroleerde voertuigen correct was geselecteerd op basis van het profiel.[27]

Bovengenoemde uitwerking is sterk gericht op sensoren die gebeurtenissen in de fysieke wereld waarnemen. Voor de volledigheid moet ook worden gewezen op het realtime detecteren van criminaliteit die online plaatsvindt of die kan worden afgeleid uit digitale communicatie die wordt onderschept. Hierbij kan onder andere worden gedacht

23 Zie Mehlbaum et al. (2014) over de verschillende betekenissen die het begrip 'heterdaadkracht' heeft. Ik bedoel het hier uitsluitend in de betekenis van 'boeven vangen'.
24 Ferguson 2022; Rienks 2015; Simmons 2019.
25 Zie ook Joh 2016.
26 Simmons 2019: 184.
27 Hierbij is het overigens nog wel de vraag wat 'correct' is, maar dit heb ik op basis van de documentatie niet kunnen vaststellen.

aan het overnemen van het beheer van dark markets door de politie[28] of het live meelezen van cryptocommunicatiedata (zie hoofdstuk 12). Ook deze verschijningsvormen van realtime detectie kunnen worden gebruikt om daders van criminaliteit op heterdaad aan te houden. Tijdens de betreffende operaties is dat ook veelvuldig gebeurd.

Samenvattend: datagedreven politiewerk kan bijdragen aan het realtime detecteren van meer strafbare feiten en vergroten van de pakkans van daders. Indien deze potentie wordt waargemaakt, heeft dit veel meerwaarde, want het 'achteraf' opsporen van verdachten is in de regel minder effectief en tijdsintensiever dan op heterdaad aanhouden.[29] Er zijn zeker voorbeelden en daarmee indicaties dat datagedreven politiewerk bijdraagt aan detectie en vergroting van de pakkans, maar meer systematisch onderzoek is nodig om hier onderbouwde uitspraken over te kunnen doen.

Tegenhouden van criminaliteit
Het tegenhouden van criminaliteit heeft betrekking op interveniëren op fenomeenniveau in plaats van incidentniveau, gericht op het reduceren of in ieder geval beheersbaar houden van het betreffende fenomeen. Ik richt me hier vooral op de georganiseerde criminaliteit. Effectiviteit wil in het licht van tegenhouden zeggen dat de uitvoering van criminele processen dusdanig door de politie (en anderen) wordt verstoord dat het moeilijker wordt om de betreffende delicten te plegen. Dit leidt idealiter tot een (tijdelijke) afname van het betreffende fenomeen, al kan het beheersbaar houden ervan veelal ook als effectief worden gezien. Het mechanisme van tegenhouden vindt plaats door 1) inzicht te krijgen in het criminele proces dat wordt uitgevoerd en de criminele netwerken die zich hiermee bezighouden, en 2) op basis hiervan interventies te bedenken en uit te voeren die het criminele proces daadwerkelijk en idealiter ook enigszins duurzaam verstoren.[30] Deze interventies kunnen het karakter hebben van het opwerpen van barrières in het proces – bijvoorbeeld in het productieproces van drugs of in technische aspecten van de uitvoering van digitale criminaliteit – maar ook van het aanhouden van subjecten uit criminele netwerken die dusdanig moeilijk vervangbaar zijn dat de uitvoering van het criminele proces (in ieder geval tijdelijk) wordt verstoord.

De bijdrage van datagedreven politiewerk aan het tegenhouden van georganiseerde criminaliteit heeft vooral betrekking op het verkrijgen van het inzicht, ook wel veiligheidsanalyse genoemd (zie hoofdstuk 18): het beeld van de criminele processen en

28 Zie Oerlemans & Van Wegberg 2019.
29 Van Os, Van den Brink & Baardewijk 2007. Bij dit onderzoek zijn wel enkele kritische kanttekeningen te plaatsen (zie Mehlbaum et al. 2014), maar die nemen niet weg dat de algemene conclusie nog steeds gerechtvaardigd lijkt.
30 Zie ook Van den Eeden et al. 2021.

daarbij betrokken subjecten.[31] Deze bijdrage bestaat meer concreet uit het eenduidig classificeren, opslaan en analyseren van data met behulp van geavanceerde technologie. De potentie van datagedreven politiewerk is dat het zorgt voor een beter beeld dan voorheen dat meer aangrijpingspunten voor interveniëren biedt. Deze potentie – wordt naar mijn indruk – op dit moment gerealiseerd. Er is een beter inzicht dan voorheen. Datagedreven politiewerk kan op dit moment niet of nauwelijks een bijdrage leveren aan de stap van beeld (hoe ziet het probleem eruit) naar interventiestrategie (hoe gaan we het aanpakken). Er is in wetenschappelijk onderzoek wel geëxperimenteerd met het gebruik van datawetenschappelijke methoden om de effecten van interventies in te schatten en zodoende afwegingen te maken.[32] Deze experimenten hebben mijns inziens nog niet geleid tot een robuuste en in de praktijk toepasbare manier van 'datagedreven interventie-ontwerp'. Het is wel denkbaar dat dit in de toekomst wordt gerealiseerd.

Kortom: datagedreven politiewerk kan bijdragen aan het in de praktijk brengen van een probleemgerichte aanpak van georganiseerde criminaliteit door de analyse van het veiligheidsprobleem te verbeteren en op basis hiervan te interveniëren.[33] Met name in de aanpak van digitale criminaliteit hebben operaties plaatsgevonden die hebben geleid tot daadwerkelijke verstoring van criminele processen – zie hiervoor hoofdstuk 18 – al is onduidelijk hoe duurzaam deze verstoring is. Ook in de aanpak van de georganiseerde (drugs)criminaliteit vindt verstoring plaats, maar ook hier is de vraag hoe duurzaam deze verstoring is. Duidelijk is in ieder geval wel dat de georganiseerde (cyber)criminaliteit een 'serieuze opponent' is die over veel adaptief vermogen beschikt.[34] Criminele sleutelspelers die worden aangehouden en vervolgd, worden snel weer vervangen door andere spelers.[35] Daarnaast kan er om barrières worden heen gewerkt. Je kunt precursoren voor de productie van synthetische drugs verbieden, maar dan schakelt men over naar precursoren.[36] Je kunt grote dark markets offline halen, maar dan schakelt men over naar kleinere markten of naar Telegram Messenger (zie ook hoofdstuk 7). Ik verwacht niet dat datagedreven politiewerk leidt tot het duurzaam reduceren van specifieke vormen van (georganiseerde) criminaliteit. Dit is naar mijn idee ook geen realistische lat om voor de politie te hanteren. Bij probleemgerichtheid gaat het er vooral om dat de politie er alles aan doet wat redelijkerwijs van haar mag worden verwacht om criminaliteits- en onveiligheidsproblemen terug te dringen en beheersbaar

31 Voor de volledigheid: een veiligheidsbeeld heeft een bredere meerwaarde dan te dienen als basis voor een strategie van tegenhouden. Een veiligheidsbeeld kan bijvoorbeeld ook worden gebruikt om incidenten die plaatsenvinden – bijvoorbeeld het aantreffen van een persoon die is overleden – in een context te plaatsen. Als je bijvoorbeeld ontdekt dat degene die is overleden onderdeel is van een crimineel netwerk, dan helpt dit bij het ontwikkelen van scenario's over wat er is gebeurd en wie daar mogelijk bij betrokken zijn. Zie ook hoofdstuk 18.

32 Barros et al. 2022; Duijn 2016; Keijser, Veldhuis & Huisman 2020.

33 In dit geval valt datagedreven politiewerk min of meer samen met intelligencegestuurd politiewerk (zie hoofdstuk 22).

34 Barros et al. 2022; Meershoek 2018; Scherpenisse, Van Twist & Schram 2017; Tops & Tromp 2017.

35 Duijn, Kashirin & Sloot 2014; Swinkels & Van Zwieten 2022.

36 Zie ook Landman, Kouwenhoven & Brussen 2020.

te houden.[37] Aan het realiseren van deze verwachting kan datagedreven politiewerk vermoedelijk bijdragen.

Ophelderen van criminaliteit
Het ophelderen van criminaliteit heeft betrekking op het reconstrueren van gepleegde strafbare feiten, zodat verdachten kunnen worden geïdentificeerd, aangehouden en vervolgd.[38] Effectiviteit wil in het kader van ophelderen zeggen dat het aandeel strafbare feiten dat kan worden gereconstrueerd en tot identificatie en aanhouding van een of meer verdachten leidt, toeneemt. De potentiële bijdrage van datagedreven politiewerk aan de effectiviteit in termen van het ophelderen van criminaliteit vindt op hoofdlijnen op een drietal manieren plaats.

Het gaat in de eerste plaats om het toenemend aantal sensoren waarmee de handel en wandel van burgers wordt waargenomen en de voortschrijdende dataficatie door sensorgebruik van burgers zelf, die ertoe leiden dat er in potentie heel veel gegevens zijn waarmee gepleegde stafbare feiten kunnen worden gereconstrueerd. Zo bevatten digitale sporendragers en digitale sporen op dit moment al een schat aan informatie waarmee scenario's over misdrijven kunnen worden gevormd, aangepast en getoetst.[39] De waarnemingen van sensoren en verzamelde datapunten functioneren bij elkaar opgeteld in toenemende mate als een 'tijdmachine'. Op het moment dat er ergens criminaliteit is gepleegd, kan er in potentie – en in ieder geval op onderdelen – worden 'teruggespoeld'. 'Crime can be investigated by rolling back digital trails', zo stelt Andrew Ferguson.[40] Hoe meer burgers 'slimme' apparaten gaan gebruiken, des te meer de dataficatie toeneemt. Hierdoor kan het internet der dingen resulteren in het *internet van bewijs*.[41]

Het gaat in de tweede plaats om de beschikbaarheid van allerlei analyse- en zoektools voor (digitaal) forensisch onderzoek. Hoe sneller uitkomsten van DNA-analyse en analyse van bijvoorbeeld gegevensdragers aan de informatiepositie in het opsporingsonderzoek kunnen worden toegevoegd, hoe groter de kans dat verdachten snel kunnen worden geïdentificeerd en aangehouden. Een bijkomend voordeel is dat andere (tactische) opsporingsmethoden niet meer hoeven te worden ingezet. In de praktijk doen de voordelen van snelle beschikbaarheid van uitkomsten van forensisch onderzoek zich ook voor, zo blijkt uit onderzoek naar experimenten en proeftuinen met het gebruik van mobiele DNA-analyse (zie hoofdstuk 11).

37 Deze uitwerking baseer ik op Terpstra 2010a.
38 De definitie van ophelderingspercentage (CBS): Het aantal misdrijven waarbij ten minste één verdachte bij de politie bekend is, ook al is deze voortvluchtig of ontkent hij/zij het strafbare feit te hebben gepleegd, gerelateerd aan het totaal aantal geregistreerde misdrijven.
39 Henseler & De Poot 2020.
40 Ferguson 2020b: 51.
41 Ferguson 2020b.

Het gaat in de derde plaats om het combineren van stukjes data: geavanceerde softwareprogramma's – zoals Palantir (zie hoofdstuk 13) – bieden de mogelijkheid om data effectief en efficiënt te doorzoeken en te analyseren. Relevante stukjes data kunnen (snel)[42] worden gevonden én aan elkaar worden verbonden. Of anders gezegd: deze programma's helpen bij het eerdergenoemde 'terugspoelen' – bijvoorbeeld door het (automatisch) visualiseren van een tijdlijn – en dit is zeer wenselijk als het om veel data gaat. Ik citeer een teamchef van de politie om dit punt nader te concretiseren.

> *'Nu zijn wij in staat om een drone de lucht in te laten. Die gaat boven het ongeluk hangen en wordt zo geprogrammeerd dat hij de kruising 3D inmeet. Die gegevens stoppen we in een softwaresysteem. Dat doen we ook met de data uit auto's en verkeerslichten. Hoewel we never nooit getuige waren van de aanrijding, kunnen we die zo wel reconstrueren.'*[43]

Kortom: door gebruik te maken van opkomende technologieën kunnen data worden gecombineerd en worden geanalyseerd ten behoeve van het reconstrueren van een gepleegd misdrijf. In de data kunnen (al dan niet ondersteunende) bewijsmiddelen worden gevonden. Deze bewijsmiddelen worden vervolgens opgenomen in het procesdossier dat wordt gebruikt voor de vervolging van verdachten.

Het voorgaande leidt tot de hypothese dat datagedreven politiewerk bijdraagt aan verhoging van het ophelderingspercentage[44] in de opsporing en aan de efficiëntie[45] van de opsporing.[46] Er zijn in de praktijk meer en minder onderbouwde aanwijzingen dat deze hypothese klopt, maar het is wederom te vroeg om hier een definitieve conclusie over te trekken.

Potentie van datagedreven politiewerk

Op basis van dit hoofdstuk trek ik de conclusie dat datagedreven politiewerk potentie heeft. Dit wil zeggen dat het kan bijdragen aan het voorkomen, detecteren, tegenhouden en ophelderen van criminaliteit. 'Kan bijdragen', want of het bijdraagt weten we op dit moment niet of nauwelijks. Er zijn zowel beloftevolle als teleurstellende voorbeelden, maar het ontbreekt aan voldoende onderzoek. Het onderzoek dat is verricht, heeft

42 Handmatig doorzoeken en analyseren van gegevens is in toenemende mate eigenlijk een onmogelijke opgave. De analist of rechercheur verdwaalt simpelweg in de data.

43 https://www.ad.nl/gouda/moordonderzoek-in-3d-animatie-laat-rechercheurs-zien-hoe-misdaad-is-gepleegd (voor het laatst geraadpleegd op 10 augustus 2023).

44 Het ophelderingspercentage is een gebrekkige prestatie-indicator voor haalcriminaliteit – zoals drugscriminaliteit – terwijl ook de opsporing van haalcriminaliteit door de beschreven werkingsmechanismen effectiever kan worden. Het gebruik van cryptocommunicatiedata is hiervan een goed voorbeeld (zie hoofdstuk 12).

45 Bij de efficiëntie moet worden opgemerkt dat dit niet zomaar betekent dat de politie meer opsporingsonderzoeken kan uitvoeren. De toenemende omvang van gegevens in opsporingsonderzoeken maakt nu eenmaal dat opsporingsonderzoek – ook met gebruik van technologie – arbeidsintensief is. Om de efficiëntie te beoordelen, moet er niet worden vergeleken met voorheen, maar met het uitvoeren van opsporingsonderzoek zonder geavanceerde analysesoftware.

46 Zie ook Hirsch Ballin & Oerlemans 2023.

vooral betrekking op predictive mapping dat naar mijn mening vooralsnog eerder als een teleurstelling dan als een belofte kan worden beschouwd.[47]

Kortom: het blijft vooralsnog bij potentie.[48] Voor het realiseren van de potentie van datagedreven politiewerk is de laatste fase van het operationele model essentieel: de aanpak op basis van het inzicht. Als betere inzichten niet leiden tot andere manieren van werken en andere operationele strategieën, dan zijn andere maatschappelijke opbrengsten ook niet waarschijnlijk. Dit vraagt sociale innovatie (zie ook hoofdstuk 23):[49] anders kijken, anders denken en anders doen, zodat er met meer creativiteit kan worden gewerkt aan de aanpak van criminaliteit.

De conclusie dat datagedreven politiewerk potentie heeft, wil niet direct zeggen dat we dit politiemodel ook moeten toejuichen. Effectiviteit en efficiëntie zijn niet de fundamenten van de rechtsstaat.[50] De potentie van datagedreven politiewerk gaat hand in hand met het risico van aantasting van (andere) publieke waarden.[51] In de volgende hoofdstukken staan de maatschappelijke risico's van de ontwikkeling naar datagedreven politiewerk centraal. Ik ga in op privacy, gelijke behandeling en het evenwicht der machten.[52]

47 Het is daarom ook jammer, en ook wel bezwaarlijk, dat wetenschappers uitspraken over de potentie van datagedreven politiewerk (big data policing) baseren op onderzoek naar predictive mapping.

48 Het duurzaam reduceren van criminaliteit is naar mijn idee geen realistische maatstaf voor datagedreven politiewerk, omdat op deze reductie factoren van invloed zijn die door uitvoering van politiewerk niet of nauwelijks kunnen worden beïnvloed (zie bijvoorbeeld Bayley, 1994; Manning, 2008).

49 Zie van Gelder 2022 voor een meer uitgebreide definitie.

50 Zie Februari 2023.

51 Hierbij moet worden opgemerkt dat datagedreven politiewerk een verzamelterm is voor uiteenlopende technologiepraktijken. Voor de risico's geldt hetzelfde als voor de opbrengsten of potentie: deze verschillen per type toepassing (zie ook Marx, 2016; Wessels, 2023). Deze risico's – net als de opbrengsten – per type toepassing kunnen verschillen. Datagedreven politiewerk is een verzamelterm. In de hoofdstukken over privacy en gelijke behandeling zal ik zo veel mogelijk specificeren welke toepassingen en risico's het betreft.

52 Ik ga dus niet in op alle relevante mensenrechten. Zo ontbreekt in dit boek een behandeling van de gevolgen van datagedreven politiewerk (en dan vooral opsporing) voor het recht op een eerlijk proces, zoals vastgelegd in artikel 6 van het EVRM. Zie hiervoor o.a. Schermer en Oerlemans (2022) en Te Molder (2022). Ik ga ook niet in op het recht op vrijheid van meningsuiting. Dit recht is wel relevant in verband met datagedreven politiewerk, in het bijzonder vanwege monitoring van sociale media en daarop gebaseerd optreden (zie hoofdstuk 16).

27 Privacy

In artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) en artikel 10 (e.v.) van de Grondwet van Nederland is het recht op eerbiediging van de persoonlijke levenssfeer opgenomen. Dit wordt ook wel het recht op privacy genoemd. De doelstelling van dit burgerrecht is het individu te beschermen tegen willekeurige inmenging door onder andere de overheid in diens privéleven of positief geformuleerd: het is het recht om met rust gelaten te worden.[1] Het verzamelen en verwerken van gegevens over een persoon is een vorm van inmenging in het leven van die persoon.[2] Dit hoofdstuk behandelt de invloed van het gebruik van opkomende technologieën in het politiewerk op de privacy van burgers. Het hoofdstuk start met een toelichting op de gevolgen van technologiegebruik voor het karakter van surveillance door de politie. Vervolgens wordt ingegaan op de hoofdlijnen van het juridisch kader dat relevant is in verband met privacy-inbreuken door de politie. Daarna komen de risico's van datagedreven politiewerk aan bod.

Digitale surveillance en doelgroepen

De politie staat in het kader van haar taakuitvoering voor de opgave om activiteiten van burgers zichtbaar te maken (zie hoofdstuk 21). Deze surveillance vindt in toenemende mate plaats met behulp van digitale technologie. Deze digitale surveillance verschilt fundamenteel van traditionele surveillance.[3] Digitale vormen van surveillance zijn meer continu en grootschaliger dan traditionele surveillance. Een softwareprogramma dat berichten op sociale media scant op basis van trefwoorden heeft een heel ander bereik dan een politiemedewerker die enkele platformen en personen langsgaat. Camera's nemen continu waar, terwijl observatie door politiemensen tijdsgebonden is. Het doorzoeken van grote hoeveelheden cryptocommunicatiedata op strafbare feiten en verdachten is iets heel anders dan op basis van een signaal een opsporingsonderzoek starten om bewijs tegen een enkele verdachte te verzamelen. Deze voorbeelden illustreren dat digitale surveillance iets anders is dan traditionele surveillance.

1 Bouteca et al. 2020; Tazelaar 2017.

2 Het recht op gegevensbescherming schaar ik in dit hoofdstuk voor het gemak onder het recht op privacy, omdat het er sterk mee samenhangt. Het recht op gegevensbescherming is een apart recht in onder andere het Handvest van de Grondrechten van de EU en in de Grondwet (zie Schermer, 2022).

3 Ferguson 2022; Marx 2016.

> *'Digital technologies alter the act of surveillance. In allowing for a broader, deeper, faster, cheaper, more accurate, automated, and aggregated process of over-collection of personal data, the thing that is happening is far different from a singular or simple collection of particularized information that human officers attempted in the past.'*[4]

Door digitale surveillance nemen de *omvang* en *diepgang* van surveillance toe.[5] Omvang verwijst naar het aantal burgers waarover de politie data verzamelt: de ogen van de politie zien steeds meer. Er is reden om aan te nemen dat de omvang van surveillance de komende jaren verder toeneemt. Niet alleen door eigen investeringen in sensoren in de fysieke wereld en (geautomatiseerde) online gegevensvergaring, maar ook door gebruik te maken van de dataverzameling van anderen in de 'slimme stad' (zie ook hoofdstuk 20). De slimme stad is dus ook een surveillance stad.[6] Deze surveillance heeft in toenemende mate een onzichtbaar karakter, omdat sensoren onderdeel zijn van allerlei 'dingen' zonder dat we hier weet van hebben. Deze onzichtbaarheid geldt des te meer voor online surveillance.[7] Burgers weten niet welke handelingen op het internet tot welke datapunten leiden en welke datapunten voor welke doeleinden worden gebruikt.[8] Dit proces van toenemende onzichtbaarheid wordt in de internationale literatuur ook wel aangeduid als de *softening* van surveillance.[9]
Diepgang heeft betrekking op het inzicht dat de politie door middel van dataverzameling en -verwerking over (bepaalde) burgers verkrijgt. Digitale surveillance leidt tot toenemende diepgang, omdat technologie wordt gebruikt bij het combineren van data uit verschillende bronnen en het leggen van verbanden tussen deze data.[10] Dit wil zeggen dat er door data te combineren een steeds gedetailleerder inzicht in de handel en wandel van burgers wordt verkregen. Ieder (persoons)gegeven op zichzelf geeft wellicht nog niet zoveel inzicht, maar het resultaat van het combineren en analyseren doet dit wel. 'The result of what you get is just vastly deeper, broader, thicker, and more revealing', aldus Andrew Ferguson over *digital policing*.[11]

Kortom: digitale surveillance is wezenlijk anders dan traditionele surveillance met als gevolg dat de omvang en diepgang van surveillance toenemen. De toenemende omvang en diepgang van surveillance gaan gepaard met het risico van meer (vergaande) inmenging van de politie in het privéleven van burgers. In het vervolg van dit hoofd-

4 Ferguson 2022: 22-23.
5 Brayne 2021.
6 Ferguson 2020b.
7 WRR 2016.
8 Dit wordt ook wel de transparantie-paradox genoemd: partijen die data verzamelen en ermee sturen weten steeds meer over burgers, terwijl burgers steeds minder weten over de praktijken van deze partijen (Friedman, 2017; ROB, 2021). Zie ook hoofdstuk 29 over transparantie.
9 Marx 2016. De term 'softening' wordt gebruikt omdat het niet alleen gaat om toenemende onzichtbaarheid, maar ook om het gegeven dat de surveillance meer onderdeel is geworden van dagelijkse activiteiten (bijvoorbeeld surfen op het internet) en daarmee een minder (direct) dwingend karakter heeft dan bijvoorbeeld surveillance door politieagenten die in de buurt rondrijden of lopen.
10 Brayne 2021; Ferguson 2022.
11 Ferguson 2022: 25.

stuk wordt nader ingegaan op deze inmenging en de rechtmatigheid van deze inmenging. Om dit te kunnen doen, is het van belang onderscheid te maken tussen verschillende doelgroepen waarover data worden verzameld en verder worden verwerkt.

> *'Police surveillance technologies are best thought of as a series of concentric circles with overlapping capabilities focused on the targets of criminal prosecution. From the outer circles of pure monitoring capabilities, to inner rings of investigation through indirect acquisition of consumer data or direct digital surveillance, to the evidentiary use of forensic data in trial, the technologies look like a bulls-eye with criminal suspects in the center.'*[12]

Het beeld van de concentrische cirkels is bruikbaar voor het maken van onderscheid in doelgroepen. In de binnenste ring bevinden zich verdachten van strafbare feiten. In de buitenste ring bevinden zich burgers van wie iets wordt vastgelegd, bijvoorbeeld omdat ze een ANPR-camera passeren. In de cirkel daartussen bevinden zich burgers die (nog) niet worden verdacht van een strafbaar feit, maar waarover wel meer data worden verzameld en/of worden verwerkt, omdat zij door de politie en/of andere partijen als een hoog risico worden beschouwd. In dit hoofdstuk ga ik vooral in op de invloed van datagedreven politiewerk op de privacy van verdachte burgers en risicoburgers.[13] Op beide typen burgers is een andere regulering van de inbreuk op hun privacy van toepassing. Dit leidt er onder andere toe dat digitale surveillance bij iedere doelgroep met eigen problemen op het gebied van rechtmatigheid gepaard gaat. Daarom behandel ik hierna de hoofdlijnen van het juridisch kader.

Privacy van burgers en juridische aspecten

Het recht op privacy is geen absoluut recht.[14] De handhaving van de openbare orde en het voorkomen en opsporen van strafbare feiten zijn zwaarwegende belangen die voor de overheid aanleiding kunnen zijn om inbreuk te maken op het recht op privacy van burgers. In de belangenafweging tussen het recht op privacy en deze overheidsbelangen vormt artikel 8 EVRM een belangrijke toetssteen. Een inbreuk op het recht op privacy in verband met deze belangen is legitiem als de inbreuk een legitiem doel dient, noodzakelijk is in een democratische samenleving en bij wet is voorzien. De inbreuk moet in verhouding staan tot het beoogde doel (proportionaliteit) en er mag geen minder ingrijpend middel zijn dat kan worden gebruikt om hetzelfde resultaat te behalen (subsidiariteit). Het criterium 'bij wet voorzien' bestaat uit verschillende uitgangspun-

12 Idem: 17.

13 De derde categorie – de buitenste cirkel – kan worden betiteld als een reguliere burger waarover gegevens worden verzameld. Hierbij kan worden gedacht aan het kenteken via een ANPR-camera (i.v.m. eventuele opsporing), videobeelden via een drone (bijvoorbeeld van jouw tuin), het gebruik van gezichtsherkenningstechnologie of sociale mediagegevens via online monitoring. Hoewel ook hier privacykwesties aan de orde zijn en er juridische vragen zijn (o.a. over de reikwijdte van artikel 3 van de Politiewet), heb ik ervoor gekozen de nadruk te leggen op de andere categorieën.

14 Deze alinea is in belangrijke mate gebaseerd op Schermer 2022.

ten, waaronder dat er (voor de inbreuk) een basis moet zijn in een nationale wet. Met betrekking tot het politiewerk gaat het dan primair om:

- Politiewet (Pw);
- Wetboek van Strafvordering (Sv);
- Wet politiegegevens (Wpg).

In de Politiewet zijn de taken, de organisatie en het beheer van de politie beschreven. In het kader van dit hoofdstuk is vooral artikel 3 Pw van belang. In dit artikel zijn de taken van de politie opgenomen (zie ook hoofdstuk 26). De politie is ter uitvoering van haar taken bevoegd tot het verrichten van alle handelingen die nodig zijn voor een goede taakuitvoering, binnen de wettelijke grenzen. Op basis van artikel 3 Pw mogen opsporingsambtenaren[15] van de politie inbreuk maken op de privacy van burgers. Op basis van artikel 3 Pw is echter alleen *een niet meer dan geringe inbreuk* toegestaan.[16] Hierbij kan in 'traditionele' zin worden gedacht aan onder andere het niet stelselmatig observeren van personen, het betreden van een voortuin en buurtonderzoek. Voor het maken van een dergelijke geringe inbreuk op de privacy van burgers is (dus) geen *specifieke*, wettelijke basis vereist.[17]

Het Wetboek van Strafvordering heeft betrekking op de opsporing en vervolging van strafbare feiten. Ik richt me hier op de opsporing. Onder opsporing wordt in het wetboek verstaan (artikel 132a Sv): het onderzoek in verband met strafbare feiten onder gezag van de officier van justitie met als doel het nemen van strafvorderlijke beslissingen. Hierbij moet worden opgemerkt dat de formulering 'in verband met strafbare feiten' geen specifieke afbakening heeft. Er bestaat in de praktijk onzekerheid over de vraag in hoeverre de fase voorafgaand aan de verdenking van een burger onder het opsporingsbegrip en daarmee onder het strafvorderlijke toezicht valt.[18] In het kader van de opsporing heeft de politie bijzondere opsporingsbevoegdheden waarmee gegevens kunnen worden verzameld. Deze bevoegdheden kunnen worden ingezet ten behoeve van onderzoek naar een gepleegd misdrijf (titel IVa) of wanneer er sprake is van een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren (titel V).[19] Met inzet van

15 Dit geldt alleen voor politiemensen die zijn aangesteld als algemeen opsporingsambtenaar. Politiemensen die zijn aangesteld als bijzonder opsporingsambtenaar (boa) hebben een specifieke, afgebakende taak waarvoor zij zijn opgeleid en een – daarmee samenhangende – beperkte opsporingsbevoegdheid.

16 In dit verband wordt vaak verwezen naar het Zwolsman-arrest uit 1995. In dit arrest heeft de Hoge Raad aangegeven dat de algemene taakstelling van de politie (toen nog opgenomen in artikel 2 Pw) voldoende grondslag biedt voor beperkte inbreuken op de persoonlijke levenssfeer. Zie http://arresten.eu/strafrecht/hr-19-12-1995-nj-1996-249-zwolsman/ (voor het laatst geraadpleegd op 13 oktober 2022).

17 Het legaliteitsbeginsel is hierbij het uitgangspunt: bevoegdheden die een ernstige inbreuk maken op de rechten en vrijheden van burgers moeten helder in de wet zijn beschreven met bijpassende waarborgen. Op basis hiervan kan het optreden worden getoetst. Voor handelingen die een geringe inbreuk maken, geldt dit dus niet.

18 Van Schendel & Cuijpers 2023; zie ook Das & Schuilenburg 2018.

19 Bijzondere opsporingsbevoegdheden kunnen ook worden ingezet bij aanwijzingen dat een terroristisch misdrijf wordt gepleegd. Zie ook hoofdstuk 24 over het steeds meer proactieve karakter van politiewerk.

deze bevoegdheden maakt de politie een meer dan geringe inbreuk op de persoonlijke levenssfeer van de betreffende burgers. Een meer dan geringe inbreuk wil zeggen dat er *een min of meer volledig beeld* wordt verkregen van (aspecten van) het leven van de betrokken burgers. Voorbeelden van bijzondere opsporingsbevoegdheden zijn onderzoek van telecommunicatie ('tappen'), stelselmatige observatie en het opnemen van vertrouwelijke communicatie (OVC). Bijzondere opsporingsbevoegdheden hebben een specifieke wettelijke basis. Voor de inzet is een bevel nodig van de officier van justitie of de rechter-commissaris. Het Wetboek van Strafvordering is gemoderniseerd. Een van de redenen voor modernisering is de digitalisering van de samenleving en de gevolgen hiervan voor het gebruik van opsporingsmethoden. In het gemoderniseerde wetboek wordt bijvoorbeeld een nieuwe bevoegdheid opgenomen ten behoeve van het overnemen van gegevens uit publiek toegankelijke bronnen (zie hoofdstuk 16). Het gemoderniseerde wetboek wordt naar verwachting in 2026 van kracht.

De Pw en het Wetboek van Strafvordering reguleren in het kader van datagedreven politiewerk *vooral* de fase van dataverzameling.[20] De mate waarin politiewerk inbreuk maakt op de privacy van burgers is bepalend voor de vraag of er specifieke opsporingsbevoegdheden nodig zijn. De politie mag door de bank genomen alleen een meer dan geringe inbreuk op de privacy van een burger maken wanneer die burger wordt verdacht van een gepleegd strafbaar feit.

De fasen van opslaan en analyseren worden vooral[21] gereguleerd door de Wpg.[22] De Wpg heeft betrekking op het verwerken van politiegegevens.[23] Elke handeling die met een politiegegeven wordt verricht, is een verwerking. Dit impliceert dat verwerken breed moet worden opgevat, waaronder: verzamelen, vastleggen, bewaren, combineren en verspreiden.[24] De Wpg kent een aantal algemene beginselen of uitgangspunten die veelal ook zijn terug te vinden in de Algemene verordening gegevensbescherming

20 In het Wetboek van Strafvordering zijn ook enkele bepalingen opgenomen die betrekking hebben op de verdere verwerking, in het bijzonder artikel 126dd Sv (zie hiervoor Fedorova et al., 2022; Hirsch Ballin & Oerlemans, 2023).

21 Naast de Wpg is er de Wet justitiële en strafvorderlijke gegevens (Wjsg). Deze is voor de politie minder relevant dan de Wpg en laat ik om die reden buiten beschouwing.

22 Dit deel van de paragraaf is in belangrijke mate gebaseerd op Franken 2017 en op de memorie van toelichting op de Wpg uit 2005.

23 Een politiegegeven is een gegeven dat te herleiden is tot een geïdentificeerd of identificeerbaar natuurlijk persoon en dat in het kader van de politietaak wordt verwerkt. Dit betreft bijvoorbeeld naam, adres, kenteken, maar ook een foto of vingerafdrukken (die tot identificatie kunnen leiden).

24 Oerlemans 2017b.

(AVG). Dit betreft in het bijzonder: noodzakelijkheid,[25] doelbinding,[26] rechtmatigheid,[27] proportionaliteit,[28] subsidiariteit[29] en dataminimalisatie.[30]

In de Wpg zijn verwerkingsgrondslagen opgenomen. Een verwerkingsgrondslag is de basis waarop een politiegegeven mag worden verwerkt. Er zijn zes grondslagen met ieder eigen voorwaarden voor onder andere verwerkingstermijnen en het ter beschikking stellen aan anderen binnen het Wpg-domein.[31] De verwerkingsgrondslagen zijn (zeer) relevant voor datagedreven politiewerk, maar het uitgebreid behandelen ervan valt buiten het doel van dit boek. Het is van belang op te merken dat er initiële verwerkingsgrondslagen zijn – in het kader van de dagelijkse politietaak (artikel 8), uitgebreidere opsporingsonderzoeken (artikel 9) of inlichtingen (artikel 10 en 12) – en grondslagen zijn voor de verdere verwerking voor een ander doel dan waarvoor ze oorspronkelijk zijn verkregen (artikel 11 en 13). De grondslagen voor verdere verwerking zijn van belang, omdat dit uitzonderingen zijn op het principe van doelbinding. Op basis van deze artikelen is het automatisch vergelijken, gecombineerd verwerken en bij elkaar brengen van gegevens mogelijk. Dit is aan – soms strikte – voorwaarden gebonden. De artikelen 11 en 13 zijn relevant voor veel van de analysetoepassingen die in deel III zijn behandeld.

In het kader van de Wpg moet tot slot worden gewezen op artikel 7a,[32] omdat hierin is opgenomen dat een besluit dat uitsluitend op geautomatiseerde verwerking is gebaseerd[33] – en dat voor de betrokkene nadelige rechtsgevolgen heeft of hem in aanmerkelijke mate treft – is *verboden*, tenzij wordt voorzien in voorafgaande *menselijke tussenkomst* door of namens de verwerkingsverantwoordelijke en in specifieke voorlichting aan de betrokkene. Dit artikel heeft dus betrekking op het gebruik van algoritmen en stelt, kort samengevat, dat de politie niet mag optreden op basis van volledig geautomatiseerde individuele besluitvorming. Er is een *human in the loop* nodig.

Het voorgaande is niet meer dan een uiteenzetting op hoofdlijnen. Deze uiteenzetting laat zien dat datagedreven politiewerk – het verzamelen, opslaan en analyseren van data en handelen op basis van ontstane inzichten – wordt gereguleerd door uiteenlopende wetten en regels. Deze zijn onder andere bedoeld om de privacy van burgers te beschermen. Hoewel weleens wordt gesteld dat vooral de gegevens*verzameling* door de

25 Gegevens mogen alleen worden verwerkt voor zover dit noodzakelijk is voor de doeleinden die in Wpg zijn geformuleerd (de verwerkingsgrondslagen, zie verder).
26 Gegevens mogen alleen worden verwerkt voor het doel waarvoor ze zijn verzameld.
27 Gegevens mogen alleen worden verwerkt als deze rechtmatig zijn verkregen.
28 Gebruik van gegevens moet altijd in verhouding staan tot het doel.
29 Doelbereiking vindt plaats op de manier die de minste inbreuk maakt op de privacy.
30 Gegevens mogen niet bovenmatig zijn; er mogen niet te veel gegevens worden verwerkt.
31 Voor het delen van politiegegevens buiten het Wpg-domein wordt de term 'verstrekken' gebruikt. Binnen het Wpg-domein vallen de politie, de Marechaussee, de rijksrecherche, bijzondere opsporingsdiensten en ook de boa voor zover deze opsporingsgegevens verwerkt.
32 Dit artikel is gebaseerd op artikel 22 van de AVG.
33 Met inbegrip van profilering.

politie wordt gereguleerd,[34] is dit mijns inziens niet terecht. De Wpg legt de (verdere) gegevensverwerking door de politie in behoorlijke mate aan banden. Hierbij zijn twee opmerkingen van belang. De eerste is dat de Wpg meer principe- dan regelgebaseerd is.[35] Dit wil zeggen dat de bepalingen ruimer zijn geformuleerd dan in bijvoorbeeld het Wetboek van Strafvordering (regelgebaseerd). De Wpg biedt daardoor meer interpretatie- en speelruimte. De tweede opmerking is dat het toezicht op naleving van de Wpg grotendeels binnen de politie plaatsvindt met de AP in een algemene, toetsende rol.[36] Dit is een wezenlijk verschil met het optreden op basis van het Wetboek van Strafvordering dat met veel meer externe en specifieke toetsing gepaard gaat. Tot slot: voor beide wetboeken geldt dat de inhoud niet meer aansluit bij ontwikkelingen in de samenleving en de consequenties hiervan voor de politie. Het gaat dan onder andere om waarborgen bij inzet van opkomende technologieën.[37] Dit is een knelpunt dat zich in internationaal verband in allerlei domeinen voordoet: de wetgever hobbelt achter de werkelijkheid aan.[38] Dit heeft niet alleen gevolgen voor de rechtsbescherming van burgers tegen de overheid, maar ook voor de mogelijkheden die de politie heeft om haar taken effectief uit te voeren. Het mogelijk maken van een effectieve taaluitvoering is immers ook een doel van wetgeving.

Risico's voor de privacy van de verdachte burger
Ik begin met de binnenste cirkel: burgers die verdacht worden van strafbare feiten of bij wie er een redelijk vermoeden bestaat dat zij zich in georganiseerd verband bezighouden met het plegen van strafbare feiten. Bij deze doelgroep heeft de politie – op basis van het Wetboek van Strafvordering en de daarin opgenomen bijzondere opsporingsbevoegdheden – vergaande mogelijkheden om legitiem inbreuk te maken op het recht op privacy. De inzet van bijzondere opsporingsbevoegdheden is bedoeld om gegevens te vergaren teneinde strafbare feiten op te helderen. Deze gegevensvergaring moet worden onderscheiden van de verdere verwerking van gegevens, waaronder het opslaan (vastleggen) en analyseren, zoals opgenomen in het werkproces van datagedreven politiewerk.

De digitalisering van de samenleving heeft in combinatie met het technologiegebruik door de politie geleid tot een toename van de mogelijkheden tot het vergaren van gegevens.[39] Voorbeelden hiervan zijn interceptie van cryptocommunicatiedata (zie

34 Zie bijvoorbeeld de WRR 2016.
35 Te Molder 2023.
36 Schermer 2022.
37 De inzet van dergelijke technologieën vindt op dit moment onder andere plaats door bestaande wettelijke uitgangspunten en wetsartikelen te interpreteren in de context van het gebruik van nieuwe technologieën. Een voorbeeld hiervan is het inzetkader gezichtsherkenningstechnologie waarin is gesteund op de systematiek van het Wetboek van Strafvordering in combinatie met strafbare feiten uit het Wetboek van Strafrecht om (als politie) zelf een afweging te maken over de inzet van de technologie (zie Politie, 2023). Men kan zich dan niet rechtsreeks op wetgeving beroepen, maar er wel iets uit afleiden.
38 Zie ook Harari 2017.
39 Fedorova et al. 2022.

hoofdstuk 12), online gegevensvergaring (zie hoofdstuk 16) en het offline halen van bijvoorbeeld dark markets, bootersites of spoofingdiensten (zie hoofdstuk 18).[40] Deze activiteiten zijn op dit moment veelal niet gebaseerd op specifieke, op die activiteiten toegesneden, opsporingsmethoden, maar op (combinaties van) opsporingsmethoden die in het pre-digitaliseringstijdperk zijn gedefinieerd.[41] Dit is begrijpelijk, de politie moet met diens tijd mee, maar roept wel de vraag op of deze bevoegdheden voldoende passend zijn gegeven de grote inbreuk die in veel gevallen op de persoonlijke levenssfeer van de gebruikers wordt gemaakt.[42]

Daarnaast – en dit is het voornaamste punt – leiden de nieuwe mogelijkheden tot dataverzameling tot het (in toenemende mate) verzamelen van *bulkgegevens* door de politie.[43] Dit wil zeggen dat er met behulp van technologie en op basis van opsporingsbevoegdheden gegevens worden verzameld over grote en deels willekeurige groepen mensen, teneinde nog onbekende personen te identificeren die van belang zijn voor de opsporing.[44] Kenmerkend voor gegevens in bulkdatasets is dat het merendeel van de gegevens betrekking heeft op personen die geen onderwerp zijn van onderzoek.[45] Dit maakt gebruik van bulkgegevens vanuit het oogpunt van het recht op privacy gevoeliger dan gebruik van gegevens die wel te relateren zijn aan een of meer personen die al onderwerp van onderzoek zijn. De consequenties van inzet van opsporingsbevoegdheden hebben betrekking op een veel grotere groep personen dan wanneer data zich beperken tot de personen die onderwerp zijn van onderzoek of daar bijvoorbeeld intensief mee samenwerken. Bij bulkgegevens kunnen er gegevens over personen in de systemen van de politie terechtkomen[46] zonder dat daarvoor – voor elk van deze personen – een legitieme reden bestaat.[47]

40 Zie Oerlemans & Van Wegberg 2019 over Hansa.
41 Schermer 2022.
42 Het omgekeerde kan overigens ook het geval zijn. Zo gebruikt de politie de bevoegdheid tot stelselmatige informatie-inwinning voor online gegevensvergaring zonder dat er daadwerkelijk onder dekmantel wordt gefunctioneerd (zonder dat er interactie met subjecten plaatsvindt). Dit is een relatief zware bevoegdheid voor de aard van de activiteit en gegevensverzameling (zie Landman & Groothuis, 2022).
43 Fedorova et al. 2022; Galič 2022; Van Schendel & Cuijpers 2023; Schermer 2022.
44 Galič 2022.
45 Fedorova et al. 2022.
46 Hierbij moet wel worden opgemerkt dat het om allerlei verschillende situaties gaat. De cryptocommunicatiedata komen bijvoorbeeld niet zomaar in de (basis)systemen van de politie terecht. Er zijn (sub-)CAT's ingericht – zie hoofdstuk 12 – die de data beheren en de data kan alleen in bepaalde gevallen (waaronder na gebruik in onderzoek en geanonimiseerd/geabstraheerd) in andere omgevingen worden gebruikt. Voor gegevens uit in beslag genomen gegevensdragers geldt dat ze in een omgeving voor digitale opsporing terechtkomen (zie Roest, 2023).
47 Fedorova et al. 2022.

Cryptocommunicatiedata als voorbeeld van bulkgegevens

Inzet van bulkbevoegdheden is van oudsher voorbehouden aan inlichtingendiensten in het kader van de nationale veiligheid.[48] De politie heeft in de afgelopen tien jaar in toenemende mate te maken gekregen met bulkdatasets, maar beschikt niet over (specifieke) bulkbevoegdheden. De politie verkrijgt bulkdatasets in de regel ook niet via een initieel ongerichte dataverzameling, zoals wel het geval kan zijn bij inlichtingendiensten.[49] De cryptocommunicatiedata zijn hiervan het meest duidelijke voorbeeld. Deze data zijn in vrijwel alle gevallen – ANOM is een uitzondering (zie hoofdstuk 12) – verkregen via een opsporingsonderzoek naar de aanbieder van de betreffende dienst. In die onderzoeken zijn de data van gebruikers onderschept met het oog op het bewijzen van de faciliterende rol van de cryptocommunicatiedienst in de georganiseerde criminaliteit. Deze data zijn vervolgens gebruikt om in de livefase of daarna strafrechtelijk onderzoek naar gebruikers te verrichten. In sommige gevallen – zoals bij Sky ECC en Exclu – is er gedurende het opsporingsonderzoek naar de cryptocommunicatiedienst (parallel) een apart onderzoek opgestart naar de gebruikers ten behoeve van de livefase. Kortom: het initiële doel is (in formele zin) dus niet om bulkgegevens te verzamelen, maar de politie krijgt wel bulkdatasets in diens bezit. Deze sets worden door de politie logischerwijs beschouwd als een 'goudmijn' voor de opsporing.[50] De aanname is immers dat degenen die gebruikmaken van dergelijke diensten dit doen om misdrijven te plegen waarbij ook kan worden gewezen op het aantreffen van de betreffende telefoons in eerdere strafrechtelijke onderzoeken.[51] Anders gezegd: het gaat hier niet om willekeurige burgers, maar om burgers waarvan kan worden vermoed dat zij zich bezighouden met het plegen van (ernstige) strafbare feiten. Op grond van artikel 126dd uit het Wetboek van Strafvordering kunnen bulkgegevens beschikbaar worden gesteld voor ander opsporingsonderzoek.[52] De data kunnen – onder (strikte) voorwaarden – worden doorzocht om subsets van data te maken voor lopende of te starten opsporingsonder-

48 Galič 2022.
49 Zie Oerlemans 2020a.
50 Schermer & Oerlemans 2022.
51 Galič 2022.
52 Hirsch Ballin & Oerlemans 2023.

> zoeken (zie verder hoofdstuk 12).[53] Ik gebruik hier cryptocommunicatiedata als voorbeeld van bulkdatasets in de opsporing, maar vergelijkbare situaties doen zich vaker voor. In grote gegevensdragers – of verschillende gegevensdragers die tegelijkertijd in beslag worden genomen – kunnen zich naast gegevens over de verdachten ook data over allerlei andere personen bevinden, die voor intelligence of strafvorderlijke doelen relevant kunnen zijn. Een andere, veelvoorkomende situatie doet zich voor in de aanpak van cybercriminaliteit: bij het neerhalen van faciliterende infrastructuren wordt er heel veel data over gebruikers vergaard, terwijl de actie daar niet op is gericht (zie ook hoofdstuk 18). Ook deze data zijn een ongekende bron om nieuwe strafbare feiten te ontdekken en intelligence te genereren.[54]

De bulkdatasets waarover de politie beschikt, worden in de regel pas waardevol als deze gegevens verder worden verwerkt door deze te doorzoeken, te combineren met andere gegevens en te analyseren.[55] De politie moet in de data immers op zoek naar strafbare feiten en moet degenen die hierbij zijn betrokken identificeren om er nader onderzoek naar te kunnen doen (dan wel het dossier op basis van de reeds vergaarde data af te ronden). Dit heeft als gevolg dat het zwaartepunt van de inbreuk die op de privacy van de betrokkenen wordt gemaakt niet zozeer bij de vergaring ligt, maar bij de verdere verwerking.[56] Het probleem is echter dat het Wetboek van Strafvordering deze verdere verwerking niet of nauwelijks reguleert. In Nederland is deze regulering verdeeld over twee wetgevende systemen: het Wetboek van Strafvordering (focus op vergaring) en de Wpg (focus op verdere verwerking).[57] In de praktijk leidt dit ertoe dat er in het strafrechtelijke systeem vooral wordt toegezien op de vergaring. Dit is onder andere zichtbaar in de jurisprudentie met betrekking tot het gebruik van de cryptocommunicatiedata, in dit geval de EncroChat data.[58] Het betreft een zaak waarin de officier van justitie stelt dat het beroep van de verdediging op basis van de Wpg niet relevant is, omdat het geen strafvorderlijke bepaling is. De rechtbank is meegegaan

53 Te Molder et al. 2023 verwijzen naar een – wat mij betreft – belangrijk onderscheid tussen *repurposing* en *recontextualization*. Bij repurposing worden gegevens die zijn verzameld voor een bepaald doel voor een ander doel gebruikt waarbij de aard en inhoud van de gegevens worden beoordeeld op relevantie voor het nieuwe doel. Dit is aan de orde bij onder andere artikel 126dd. Bij recontextualization worden de gegevens ook voor een ander doel gebruikt dan waarvoor ze zijn vergaard, maar het karakter van dit doel is anders dan het doel waarvoor de gegevens oorspronkelijk zijn vergaard. Bij recontextualization wordt er namelijk nieuwe informatie uit afgeleid die als zodanig nog niet bekend was. Er ontstaan nieuwe inzichten die onder andere als gevolg kunnen hebben dat personen object van onderzoek worden die eerder nog niet (in die hoedanigheid) in beeld waren. Dit kan zich voordoen bij het gebruik van (onder andere) cryptocommunicatiedata ten behoeve van intelligence (zie ook hoofdstuk 18). Te Molder et al. (2023) merken op dat recontextualization in algemene zin gepaard gaat met meer privacyrisico's dan repurposing.

54 Hirsch Ballin & Oerlemans 2023.

55 Fedorova et al. 2022.

56 Fedorova et al. 2022; Galič 2022.

57 In de (concept-)memorie van toelichting bij het nieuwe Boek 2 van het Wetboek van Strafvordering is door de wetgever nogmaals benadrukt dat er een 'harde knip' bestaat tussen deze twee systemen (zie Schermer, 2022).

58 Ik baseer dit voorbeeld op van Schendel & Cuijpers 2023; zie ook Galič 2022 voor vergelijkbare constateringen met betrekking tot de oriëntatie in de strafrechtspraak (focus op vergaring).

in het betoog van de officier van justitie, omdat de Wpg geen strafrechtelijk voorschrift is.[59] De verwerking van de EncroChat data wordt hiermee niet door strafrechter beoordeeld. Dit roept de vraag op wie – op meer afstand van de opsporing[60] – wel toeziet op de bescherming van het recht op privacy in de fase van verdere verwerking. De AP heeft een algemene toezichthoudende rol met betrekking tot de Wpg, maar dat is geen toetsing in concrete gevallen in het kader van opsporing.[61] Deze toetsing ontbreekt. Dit is – gegeven de kenmerken van bulkgegevensverzameling – een knelpunt. De parallel met de vereisten die het Europees Hof voor de Rechten van de Mens (EHRM) stelt aan bulkinterceptie door inlichtingdiensten is in dit kader relevant.

Regulering van bulkbevoegdheden van inlichtingendiensten[62]
Bulkdatasets zijn voor de politiële opsporing een relatief nieuw fenomeen. Dit geldt echter niet voor inlichtingendiensten. Het is daarom van meerwaarde om een uitstap te maken naar hoe met regulering van dergelijke bevoegdheden wordt omgegaan. Ik beperk me hier tot de benadering van het EHRM. Voor de bulkbevoegdheden van de inlichtingendiensten geldt dat de Grote Kamer van het EHRM als uitgangspunt neemt dat er sprake moet zijn van 'end-to-end waarborgen'. Dit wil zeggen dat in iedere fase van het proces – het hof maakt onderscheid tussen verzamelen, selecteren, analyseren en gebruiken[63] – waarborgen moeten zijn ingebouwd, in het bijzonder met betrekking tot de noodzakelijkheid en proportionaliteit van de activiteiten. Volgens het hof neemt de mate van inmenging in de persoonlijke levenssfeer toe naarmate het proces verder vordert. Dit wil zeggen: als je personen gaat selecteren en nader gaat analyseren (onder andere door gebruik te maken van andere gegevens) teneinde tot daadwerkelijk gebruik van gegevens te komen. Het hof is in de afgelopen jaren dan ook veel meer gaan richten op het reguleren van het verwerkingsproces. Er wordt een ruime gegevensvergaring toegestaan, maar vervolgens worden wel gedetailleerde procedures en regels voor analyse, bewaring en het delen van gegevens geëist. Deze procedures en regels worden versterkt met toezichtarrangementen en de controle daarop.

59 Zie ook Hirsch Ballin & Oerlemans 2023.

60 Te Molder et al. (2023) merken op dat er in het geval van de cryptocommunicatiedata – bij gebrek aan (nadere) wettelijke normering – tamelijk *ad hoc* is gezocht naar oplossingen om toch grenzen te stellen aan het onderzoek van bulkgegevens. Dit heeft geleid tot het inschakelen van de rechter-commissaris voor het stellen van nadere voorwaarden aan de manier waarop gegevens mogen worden gebruikt en geanalyseerd (zie ook hoofdstuk 12). Onderdeel hiervan was een toetsende rol van de rechter-commissaris voorafgaand aan ieder nieuw onderzoek. Te Molder et al. (2023) benadrukken dat toetsing tijdens en na de gegevensverwerking ook noodzakelijk is. Zij pleiten voor een meer dynamische vorm van toezicht.

61 De AP kan gebruik maken van verschillende handhavende en sanctionerende bevoegdheden (zoals een last onder dwangsom of bestuurlijke boete) en doet dit ten aanzien van de politie ook weleens, maar heeft bijvoorbeeld geen bevoegdheid om bij vastgestelde onrechtmatigheden verwerkingen stil te leggen. Deze onrechtmatigheden komen ook niet zomaar aan het licht, aangezien er niet wordt getoetst in concrete gevallen (zie Fedorova et al., 2022).

62 Deze alinea is vooral gebaseerd op Galič 2022.

63 Hierbij valt op dat deze vierdeling van het hof – die is bedoeld voor *bulkinterceptie* – veel overeenkomsten heeft met hoe de politie datagedreven politiewerk operationaliseert (zie hoofdstuk 22).

Het voorgaande leidt tot de conclusie dat de introductie van bulkgegevens in het kader van de opsporing resulteert in het maken van inbreuken op de privacy van burgers die in beperkte mate op *specifieke, daarop toegesneden* wet- en regelgeving is gebaseerd.[64] Daarnaast is er beperkt ex-post toezicht op de gegevensverwerking die na de vergaring van gegevens plaatsvindt. Dit is een gevolg van het strikte onderscheid dat wordt gemaakt tussen vergaren enerzijds (Sv) en verwerken anderzijds (Wpg). Het punt is echter dat dit strikte onderscheid – op basis van de huidige en zeker toekomstige praktijk – niet meer goed te verdedigen is.[65] Het recht moet de burger integrale bescherming bieden tegen inbreuken op (onder andere) de persoonlijke levenssfeer die het gevolg is van overheidshandelen.[66] Hoewel er al heel vaak is gepleit voor het oplossen van het probleem van de strikt gescheiden wetgevende systemen, is er nog geen oplossing in gang gezet.[67] Het huidige strafvorderlijk kader biedt onvoldoende bescherming en de voorgestelde modernisering van het Wetboek van Strafvordering lost de knelpunten niet of in ieder geval onvoldoende op.[68] Hirsch Ballin en Oerlemans concluderen: 'Datagedreven onderzoek is een "game changer" voor de politie en dat zou het ook voor de relatie tussen Sv en Wpg en het bijhorende toezicht moeten zijn.'[69]

Privacy-inbreuken en de risicoburger

In hoofdstuk 6 is beschreven dat er vanaf de jaren tachtig van de vorige eeuw – vanwege de toename van criminaliteit – een veiligheidsoffensief tot stand is gekomen. Dit offensief heeft de samenleving een ander aanzien gegeven: hang-en-sluitwerk, camera's, particuliere beveiligers, veiligheidshuizen en ga zo maar door.[70] Veiligheid heeft vanaf die periode een meer 'ordende' functie in de samenleving gekregen. Dit wil onder andere zeggen dat het een dominant gezichtspunt is geworden. Dit heeft als gevolg dat (maatschappelijke) ontwikkelingen bij voortduring in termen van (on)veiligheid worden gedefinieerd.[71] Een uitvloeisel hiervan is een oriëntatie op risico voor veiligheid.[72] De terrorismedreiging heeft deze risico-oriëntatie rondom het millennium verder versterkt. Vanuit deze risico-oriëntatie is er een sterke behoefte om bedreigin-

64 Hierbij moet ook de vraag worden gesteld of de bepalingen uit de Wpg wel voldoende zijn toegesneden om als grondslag te dienen voor verwerking van bulkgegevens (zie Hirsch Ballin & Oerlemans, 2023). Wie de memorie van toelichting op de Wpg leest, zal vermoedelijk concluderen dat deze in een ander tijdsgewricht is opgesteld.

65 Fedorova et al. 2022; Hirsch Ballin & Oerlemans 2023.

66 Hirsch Ballin & Oerlemans 2023.

67 Het doel hiervan is te komen tot samenhang in de normeringskaders (zie Hirsch Ballin & Oerlemans, 2023). Fedorova et al. (2022) stellen voor om verwerkingshandelingen die zijn gericht op kennisvermeerdering én een strafvorderlijk doel dienen, in het Wetboek van Strafvordering onder te brengen en daar nader te normeren. Gegevensbescherming wordt dan geïntegreerd in het strafprocesrecht, zodat de rechter hierop (ex-post) kan toetsen (zie ook Schendel & Cuijpers, 2023). De overige verwerkingshandelingen kunnen in de Wpg worden genormeerd (zie de volgende paragraaf). Zij pleiten dus voor een onderscheid tussen strafvorderlijke en niet-strafvorderlijke gegevensvergaring en -verwerking.

68 Zie o.a. Schendel & Cuijpers 2023; Schermer 2022.

69 Hirsch Ballin & Oerlemans 2023: 36.

70 Boutellier 2020.

71 Zie ook Frissen 2022.

72 Devroe 2017.

gen op het gebied van veiligheid tijdig in te schatten en hierop te anticiperen. De politie speelt hierin een belangrijke rol. In hoofdstuk 24 is beschreven dat deze voorzorg- of anticipatielogica ertoe leidt dat de politie vaker ingrijpt voordat het kwaad is geschied. Dit is – gegeven de dominantie van risicobeheersing – zowel een verwachting van politiek en samenleving als een eigenstandig streven van de politie. Proactief optreden heeft een positieve connotatie, want voorkomen is beter dan genezen.[73]

De opkomst van de risicoburger moet tegen bovenstaande achtergrond worden begrepen. Het is – ten opzichte van de verdachte burger – een relatief nieuwe categorie. Dit is in de politiepraktijk zichtbaar: waar de politie vroeger alleen gegevens vastlegde over personen die (vermoedelijk) iets hadden gedaan of waarmee anderszins bemoeienis gerechtvaardigd was, worden er al geruime tijd ook gegevens vastgelegd over onverdachte personen.[74] De nadruk die van oorsprong ligt op gegevensverwerking van uitsluitend verdachte personen heeft onder andere te maken met het gegeven dat de politie een opsporingsinstantie is en geen inlichtingendienst. Een inlichtingendienst mag – binnen juridische kaders – over burgers al vroegtijdig gegevens verzamelen en vastleggen als men vermoedt dat deze een gevaar voor de democratische rechtsstaat kunnen vormen. Als er van daadwerkelijk gevaar sprake is, volgt er een ambtsbericht aan de politie die de opsporing ter hand neemt. De voorzorglogica heeft ertoe geleid dat de grens tussen het verzamelen van inlichtingen enerzijds en het opsporen van strafbare feiten anderzijds een minder scherpe grens is dan voorheen.[75] Dit is in de praktijk onder andere merkbaar bij online gegevensvergaring (zie hoofdstuk 16): het is waarschijnlijk dat politiemensen en medewerkers van de AIVD allebei aanwezig zijn in besloten online groepen om intelligence te vergaren, zonder dit van elkaar te weten.[76]

Bovenstaande aanloop is nodig om te kunnen duiden dat technologische ontwikkelingen niet meer zijn dan een versterker van het al bestaande veiligheidsregime van risicobeheersing. Opkomende technologieën bieden de politie (en andere partijen) de mogelijkheid om op grote(re) schaal en op efficiënte(re) wijze risico's in te schatten en op basis hiervan op te treden.[77] Dit leidt er in combinatie met actuele veiligheidsdreigingen – zoals cybercriminaliteit, georganiseerde drugscriminaliteit en maatschappelijk ongenoegen – toe dat de politie met behulp van technologie in toenemende mate gegevens verzamelt en verwerkt over burgers die (nog) geen verdachte zijn.[78] Hierbij moet worden benadrukt dat zich binnen deze categorie van onverdachte, (risico)burgers vele subcategorieën bevinden: van jongeren die nog nooit een strafbaar feit heb-

73 Het gaat dan vooral om het voorkomen van incidenten en niet zozeer om het beïnvloeden van de dieperliggende oorzaken of situationele omstandigheden van criminaliteit. Zie hoofdstuk 24.
74 Deze alinea is in belangrijke mate gebaseerd op Tazelaar 2017.
75 Zie onder andere Galič 2022; Vis 2012.
76 Zie ook Landman & Groothuis 2022.
77 Over de accuraatheid kunnen vooralsnog geen (onderbouwde) uitspraken worden gedaan en is ook veel discussie. Zie onder andere het vorige en volgende hoofdstuk.
78 Zie ook dit gesprek met hoogleraar inlichtingen en recht Jan Jaap Oerlemans: https://www.ftm.nl/artikelen/jan-jaap-oerlemans-wildgroei-inlichtingenwerk (voor het laatst geraadpleegd op 6 januari 2023).

ben gepleegd, maar wel voldoen aan risico-indicatoren tot personen waarvan de politie vermoedt dat zij criminaliteit plegen, maar waarbij dit vermoeden nog niet voldoende kan worden onderbouwd om tot opsporing over te gaan.

De kans op onrechtmatige privacy-inbreuken bij risicoburgers vloeit in de eerste plaats voort uit de gegevensverzameling. Door de toenemende omvang van surveillance kan surveillance het karakter krijgen van een sleepnet waarbij grote groepen onverdachte burgers in beeld worden gebracht om vervolgens te beoordelen welke burgers een risico vormen voor de samenleving.[79] Deze gegevensverzameling is gericht op intelligence (in plaats van bewijs) en moet in veel gevallen plaatsvinden op basis van artikel 3 Pw. De politie mag immers geen bijzondere opsporingsbevoegdheden inzetten om intelligence te vergaren, behalve wanneer er sprake is van een aanwijzing van terroristische dreiging of een redelijk vermoeden dat in georganiseerd verband misdrijven worden gepleegd (titel V onderzoek). Gegevensverzameling op basis van artikel 3 heeft als consequentie dat deze alleen een niet meer dan geringe inbreuk mag maken op de privacy van de betrokken burgers. De grens tussen een niet meer dan geringe en een meer dan geringe inbreuk is lastig te bepalen. Dit geldt in het bijzonder bij digitale surveillance, omdat de jurisprudentie die beschikbaar is voor het beoordelen van de grens betrekking heeft op het pre-digitaliseringstijdperk.[80] Deze is niet of nauwelijks bruikbaar voor digitale surveillance, omdat digitale surveillance – zoals eerder aangegeven – wezenlijk anders is dan traditionele surveillance. Er is dus weinig houvast om deze politiepraktijken te beoordelen.

De kans op onrechtmatige inbreuken door de politie op de privacy van onverdachte burgers is vooral aanwezig wanneer gegevens worden gecombineerd. Dit komt doordat de diepgang toeneemt, wat simpelweg impliceert dat een meer dan geringe inbreuk op de privacy al snel dichterbij komt. Terug naar de inleiding van dit hoofdstuk: ieder afzonderlijk gegeven geeft weliswaar geen min of meer volledig beeld van (aspecten van) het leven van een burger, maar de combinatie en analyse van gegevens kan dit wel geven.[81] Een praktijk om dit te illustreren.

Interactieve criminele kaart

In een van de politie-eenheden in ons land is geëxperimenteerd met een 'interactieve criminele kaart': een digitale beeldtafel waarop allerlei plaatsen (waaronder woonadressen en bedrijven) worden weergegeven.[82] Plaatsen worden geclassificeerd: is er iets verdachts aan de hand? Deze classificatie vindt plaats op basis van uiteenlopende data: politiedata, maar ook data van andere organisaties, zoals de Kamer van Koophandel (KvK) en het Kadaster.

79 Brayne 2021; WRR 2016.
80 Zie ook Landman & Groothuis 2022.
81 Zie ook Stevens et al. 2021.
82 https://www.politie.nl/nieuws/2019/augustus/28/08-opening-criminele-kaart-op-team-weerijs.html (voor het laatst geraadpleegd op 8 augustus 2022).

> De gebruiker kan op plaatsen en daarbinnen op individuen – aan de hand van het woonadres – inzoomen om zodoende inzicht te krijgen in onderliggende data. De criminele kaart wordt door de politie beschouwd als een aanvulling voor de politieagenten op straat. 'Wanneer hij rondrijdt ziet een agent natuurlijk niet wat er achter de deuren afspeelt, deze kaart biedt hem de mogelijkheid om eigen kennis, ervaring en inzicht te koppelen aan andere gegevens', zo valt op de website van de politie te lezen.[83] De beeldtafel wordt – bij mijn weten – gebruikt in de zogenaamde 'digikamers' van de basisteams in de eenheid.[84]

De interactieve criminele kaart of beeldtafel illustreert hoe het combineren van gegevens leidt tot meer diepgang: er wordt een min of meer volledig beeld verkregen van (aspecten van) het leven van een burger.[85] In geval van een verdachte – een specifieke verdenking – kan dit beeld worden verkregen door inzet van bijzondere opsporingsbevoegdheden en kunnen gegevens worden gecombineerd en geanalyseerd voor het doen van onderzoek in verband met strafbare feiten. Het combineren en analyseren van gegevens over onverdachte burgers is echter een andere kwestie. De rechtmatigheid van de inbreuk die op de privacy van burgers wordt gemaakt, staat dan veel meer ter discussie. Dit is in bovengenoemd voorbeeld het geval en ook bij systemen die burgers expliciet in een risicocategorie plaatsen, zoals aan de orde was in de sensing proeftuin in Roermond[86] of aan de orde is bij systemen voor predictive identification.[87] Het risico van onrechtmatigheid is reëel. Niet alleen vanwege de reikwijdte van artikel 3 Pw, maar ook en vooral vanwege de Wpg en de bepalingen die hierin zijn opgenomen met betrekking tot het automatisch vergelijken en gecombineerd verwerken van gegevens. Deze bepalingen begrenzen de fasen van combineren en analyseren, maar binnen de politie is de omgang met en correcte naleving van de Wpg – zoals eerder aangegeven (zie hoofdstuk 25) – 'lastige materie'.[88]

---

83 https://www.politie.nl/nieuws/2019/augustus/28/08-opening-criminele-kaart-op-team-weerijs.html (voor het laatst geraadpleegd op 8 augustus 2022).

84 Zie Schiks, Van 't Hoff-de Goede & Leukfeldt 2022.

85 De ambitie van diepgang klinkt ook door in de toelichting: de politie wil 'zien' wat zich achter de deuren afspeelt. Wanneer dit wordt toegepast op traditionele surveillance wordt het problematische karakter direct duidelijk, want de politie kan op basis van artikel 3 Pw niet zien wat zich achter de deuren afspeelt. Dit maakt ook duidelijk dat digitale surveillance anders is dan traditionele surveillance: je kunt al snel meer 'zien' zonder dat een burger het doorheeft.

86 Stevens et al. (2021) geven aan dat het sensing project was gebaseerd op artikel 3 Pw en artikel 8 Wpg en concluderen dat deze juridische grondslagen niet zijn toegesneden op de aard van het project (risicotaxatie op individueel niveau). Zie ook Prins (2020) die – uitgaande van het Europese mensenrechtelijke kader – eveneens concludeert dat de algemene taakomschrijving van de politie (artikel 3 Pw) onvoldoende waarborgen biedt.

87 Hierbij moet – wellicht ten overvloede – worden benadrukt dat het (al dan niet realtime) plaatsen van een burger in een risicocategorie niet automatisch kan leiden tot een redelijk vermoeden van schuld in de zin van het Wetboek van Strafvordering (zie ook Stevens et al., 2021; Ferguson, 2012 voor de VS).

88 Tazelaar 2017; zie ook Winter et al. 2020.

Bij het voorgaande moet worden benadrukt dat het niet alleen gaat om de gegevensverzameling en -verwerking als zodanig, maar ook om het optreden van de politie – de vierde fase van datagedreven politiewerk – dat op basis van deze verwerking plaatsvindt, bijvoorbeeld in de vorm van proactieve controles.[89] Dit optreden versterkt de inbreuk die wordt gemaakt; het doet afbreuk aan het recht dat de onverdachte burger heeft om door de politie met rust gelaten te worden. Hoe repressiever de interventies zijn, hoe meer burgers worden belemmerd in de uitoefening van (andere) fundamentele rechten.[90]

De opkomst van een gedachtepolitie?

De positieve connotatie van proactief politieoptreden – voorkomen is beter dan genezen – gaat gepaard met de kans dat er in toenemende mate een politie ontstaat die (ook) opereert op de grens tussen gedachten en gedragingen van burgers.[91] Ik zal dit met een voorbeeld illustreren.[92] In februari 2023 was er een burger die naar aanleiding van de megawinst van Ahold Delhaize had getweet dat het moreel acceptabel was om te stelen bij Albert Heijn, omdat er over de rug van de basisbehoeften van burgers megawinsten werden gemaakt. Dit resulteerde in een wijkagent aan de deur die aangaf dat ze een signaal had gekregen van de 'digi-afdeling'. Ze waarschuwde de burger en gaf aan dat als het 'verder zou gaan met hem', de politie zou gaan kijken wat er kan worden gedaan met het account. Ook werd aangegeven dat hij gevolgd zou worden (online). Dit voorbeeld illustreert hoe de politie op basis van intelligence aan het opschuiven (of eigenlijk terugschuiven) is op de grens tussen gedachte en gedraging. Het gevaar ontstaat dat het hebben en uiten van bepaalde gedachten steeds meer voorwerp van politiecontrole gaat worden. Dit betreft niet alleen gedachten over het (zelf) wel of niet begaan van strafbare feiten, maar ook het hebben en uiten van gedachten gericht op gedrag van anderen (zoals bij online opruiing; het voorbeeld kan wellicht worden beschouwd als een lichte vorm hiervan).[93] Digitale surveillance heeft op deze wijze niet alleen consequenties voor de privacy van

89 Das & Schuilenburg 2018.

90 Zie ook Schermer & Galič (2023) die erop wijzen dat privacy een infrastructurele rol heeft: het is niet alleen recht in zichzelf, maar ook een belangrijke voorwaarde voor de bescherming en realisatie van andere rechten en vrijheden. Zonder privacy wordt het immers moeilijk om sommige andere rechten te genieten. Mede om die reden pleiten zij ervoor om de sociale, culturele en uiteindelijk ook juridische conceptualisering van het privacyconcept – in het kader van de opkomst van datagedreven politiewerk – uit te breiden met rechten die op groepsniveau worden geformuleerd (zie ook het volgende hoofdstuk over het plaatsen van individuen in een algoritmisch samengestelde risicogroep). Dit wordt in de literatuur (onder andere) *group privacy* genoemd.

91 Zie Schuilenburg 2016.

92 Ik baseer dit voorbeeld op eigen openbronnenonderzoek, inclusief waarheidsgetrouwe videobeelden van het gesprek tussen de wijkagent en de betreffende burger.

93 Zie ook het rapport van Amnesty International (2023) over de politiële gegevensverzameling en controles van vreedzame demonstranten, waaronder het thuis opzoeken van demonstranten. Een groot risico van de nadruk op maatschappelijk ongenoegen en het risico op (onder andere) openbare-ordeverstoringen is dat de politie een demonstratie te veel gaat zien als een risico in plaats van mensenrecht.

burgers, maar ook voor de vrijheidssfeer van burgers.[94] De kans dat dergelijke vormen van surveillance en controle in de komende jaren toenemen, is groot. Het ongenoegen in de samenleving heeft zich gemanifesteerd als een nieuw veiligheidsvraagstuk (zie hoofdstuk 8). Het verzet tegen de overheid wordt door de politie in de gaten gehouden, onder andere om anti-overheidsextremisme te kunnen signaleren. Dit heeft als onvermijdelijk gevolg dat onverdachte burgers worden gemonitord en onderwerp kunnen worden van proactieve controle.[95]

Het risico op onrechtmatige privacy-inbreuken is als zodanig problematisch, maar er spelen ook nog twee andere problemen die van belang zijn. Het eerste probleem is dat er tegenover de soms vergaande inbreuken op de privacy van de risicoburger weinig rechten staan.[96] De risicoburger is geen juridische categorie, zoals een verdachte. In het strafrecht is de presumptie van onschuld een grondbeginsel: eenieder is onschuldig tot het tegendeel is bewezen. Dit (abstracte) beginsel biedt burgers bescherming tegen strafvorderlijk optreden van de Staat. Strafvorderlijk optreden mag plaatsvinden wanneer er sprake is van een redelijk vermoeden van schuld aan een strafbaar feit. Dit redelijke vermoeden moet door de politie worden onderbouwd met feiten en omstandigheden. Een officier van justitie beslist vervolgens of iemand wordt aangemerkt als verdachte. Vanaf het moment dat iemand een verdachte is, kunnen er meer ingrijpende bevoegdheden worden ingezet, bijvoorbeeld stelselmatige observatie of het (zonder toestemming) binnentreden van een woning.[97] De status van verdachte gaat echter ook gepaard met rechten, zoals het recht op een zelfgekozen raadsman of het recht om kennis te nemen van de processtukken die in de strafzaak worden gebruikt. De risicoburger heeft dergelijke rechten niet of nauwelijks.[98] Bijvoorbeeld: voor zover de risicoburger weet dat die deze status heeft gekregen, zijn er geen procedures om die status te betwisten (zie ook hoofdstuk 28).[99] De risicoburger is relatief onbeschermd.[100]

Het tweede probleem houdt (enig) verband met het eerste, maar verdient een aparte behandeling: er is niet of nauwelijks toezicht op de gegevensverzameling en -verwer-

94 Zie Schuilenburg 2016.

95 Zie bijvoorbeeld: https://www.platform-investico.nl/artikel/politie-verzamelt-op-grote-schaal-persoonsgegevens-demonstranten/ (voor het laatst geraadpleegd op 11 maart 2023).

96 WRR 2016; zie ook Brayne 2021 voor de VS.

97 Er zijn uitzonderingen, zie eerder in dit hoofdstuk.

98 Hierbij is het onderscheid tussen risicoburgers die in werkelijkheid onschuldig zijn en risicoburgers die zich wel schuldig maken aan strafbare feiten van belang. Burgers die onschuldig zijn, mogen een redelijke verwachting van privacy hebben en moeten in dat kader worden beschermd. Bij burgers die strafbare feiten plegen – maar geen verdachte zijn – is minder sprake van deze redelijke verwachting. Daarom is de accuraatheid van de risicotaxatie ook van belang. Zie ook Simmons (2019).

99 Zie bijvoorbeeld Peeters & Van Dongen (2022) over de Top600.

100 De meest vergaande consequenties hiervan doen zich voor in het domein van terrorismebestrijding wanneer je als burger onterecht op een (internationale) lijst komt te staan en hier niets van weet en weinig tegen kunt doen. Lees: https://www.ftm.nl/artikelen/terreurlijst-vervolg-politie-namen-onschuldigen-vs? (voor het laatst geraadpleegd op 10 augustus 2023).

king met betrekking tot onverdachte burgers door de politie.[101] Dit punt is ook al bij verdachte burgers behandeld, maar beperkt zich daar tot de verdere verwerking van gegevens. Bij onverdachte burgers is de situatie dus problematischer, omdat het hier ook de gegevensverzameling betreft. Er is ex-ante in de regel nog wel enig toezicht door onder andere de informatieofficier van het OM,[102] maar ex-post is dit toezicht er niet of nauwelijks.[103] Om die reden pleiten diverse experts om ook de niet-strafvorderlijke vergaring en verwerking van gegevens te normeren en hierbij – voor wat betreft de vergaring – aansluiting te vinden bij strafvorderlijke waarborgen en voorwaarden.[104]

Dit hoofdstuk gaat naar een afronding, dus daarom tot slot: mijn overtuiging is dat de datahonger[105] van de politie voortkomt uit goede bedoelingen – samengevat als het voorkomen van narigheid – maar dit wil niet zeggen dat het daarmee ook deugt en deugt doet.[106] De initiator van de Amerikaanse privacyregels, rechter Louis Brandeis, zei lang geleden (1928) al: het grootste gevaar voor de privacy ontstaat als de bedoelingen van de overheid goed zijn.[107] Dit vraagt dus alertheid op (digitale) surveillancepraktijken van zowel de politie als andere actoren.[108] Gemoderniseerde wetgeving is van belang om enerzijds de mogelijkheden van de politie te expliciteren en te reguleren en anderzijds burgers te beschermen tegen de datahonger van de politie. Er is echter meer nodig dan normering door wet- en regelgeving. Een democratische politie mag de bescherming van grondrechten niet louter als een politiek vraagstuk definiëren. De politie heeft in het beschermen van grondrechten een eigen verantwoordelijkheid. Goed politiewerk impliceert dat mensenrechten worden beschermd. Niet omdat het moet, maar omdat het hoort. Dit betreft niet alleen het recht op privacy, maar ook het recht op gelijke behandeling dat centraal staat in het volgende hoofdstuk.

101 Zie ook Koelewijn 2009.
102 Zie bijvoorbeeld Groothuis & Landman 2022.
103 Dit geldt (dus) ook voor allerlei verstoringsactiviteiten van de politie in casuïstiek die nooit voor een rechter wordt gebracht (zie hoofdstuk 18; zie ook Schermer, 2022).
104 Commissie Koops 2018; Stevens et al. 2021.
105 Deze formulering leen ik van Oerlemans (2020a) die deze voor de inlichtingendiensten heeft gebruikt.
106 Deze woorden leen ik van Jan Nap.
107 Zie https://www.nrc.nl/nieuws/2021/05/16/ambtenaren-willen-meer-dan-mag (voor het laatst geraadpleegd op 1 augustus 2021).
108 In dit verband is het van belang om te wijzen op het voorstel voor wijzing van de Wet ter voorkoming van witwassen en financieren van terrorisme (zie Ipenburg, 2023). Dit wetsvoorstel voorziet onder andere in een wettelijke grondslag voor het gezamenlijk monitoren van transacties door banken en in gegevensdeling in het kader van onderzoek van cliënten met een 'hoog risicoprofiel'. Met de gezamenlijke monitoring zullen persoonsgegevens op grote schaal worden verzameld en geanalyseerd. De AP gebruikte in een reactie op een eerdere versie van het wetsvoorstel de term 'bancair sleepnet'. Ook de Raad van State merkte op dat de massale schaal waarop monitoring gaat plaatsvinden 'ongekend' is. Naast dit wetsvoorstel ligt er ook een voorstel voor de Wet gegevensverwerking door samenwerkingsverbanden (WGS), die het mogelijk maakt om ruimer gegevens te delen in samenwerkingsverbanden in de aanpak van ondermijnende criminaliteit (zie hoofdstuk 29). Dergelijke wetsvoorstellen creëren de zorg dat we ons laten meeslepen in de richting van een surveillancestaat (zie Verhoeven, 2023).

28 Gelijke behandeling

In menig politiebureau is artikel 1 van de Grondwet zichtbaar in de ontvangsthal: 'allen die zich in Nederland bevinden, worden in gelijke gevallen gelijk behandeld. Discriminatie wegens godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht of op welke grond dan ook, is niet toegestaan'. In de (internationale) literatuur wordt toenemende discriminatie beschouwd als een van de maatschappelijke risico's van datagedreven politiewerk. In dit hoofdstuk ga ik in op deze thematiek. Het gaat dan in het bijzonder om vormen van *predictive policing* waarbij bepaalde plaatsen en individuen als risico worden getaxeerd met mogelijk intensievere politiebemoeienis als gevolg.

Valspositieven, valsnegatieven en consequenties

Algoritmische besluitvorming is niet perfect. Er wordt niet letterlijk voorspeld, er worden kansen berekend.[1] Hierbij worden fouten gemaakt: gedrag van mensen laat zich niet volledig voorspellen.[2] Er zijn er altijd valspositieven en valsnegatieven.[3] Valspositief wil zeggen dat er iets (gebied, individu) wordt aangemerkt als hoog risico, terwijl hier in werkelijkheid geen sprake van is. Valsnegatief is het omgekeerde: iets aanmerken als laag risico, terwijl het in werkelijkheid om een hoog risico gaat.[4] Neem een proactieve controle: wie handelt op basis van een valsnegatief kan een crimineel laten passeren, terwijl wie handelt op basis van een valspositief een onschuldige burger controleert die niets crimineels heeft gedaan of van plan is.

In algemene zin geldt dat de gevolgen van algoritmische besluitvorming voor het leven van burgers sterk afhangen van het doel dat met een AI-systeem wordt beoogd. Een verkeerde aanbeveling van Netflix is simpelweg een stuk minder vervelend dan onterecht te worden aangemerkt als een risicoburger die vervolgens intensiever (op wat voor manier dan ook) wordt gecontroleerd (zie ook hoofdstuk 19). Het is daarom van belang om fouten niet alleen te kwantificeren – in termen van het percentage (on)ac-

1 Februari 2023.
2 Rathenau Instituut 2021.
3 Bijlsma, Bex & Meynen 2019.
4 Ik definieer valspositief en valsnegatief hier in de context van risicotaxatie. Het is van belang te benadrukken dat beide typen fouten zich bij vrijwel alle toepassingen kunnen voordoen. Bij risicotaxatie van plaatsen, individuen en/of (verdachte) situaties is de kans op fouten groter dan bij bijvoorbeeld een programma dat automatisch afbeeldingen doorzoekt. Dit geldt in het bijzonder voor profilering (individu, situatie), omdat het om samengestelde, contextuele betekenissen gaat die relatief instabiel zijn (zie Gigerenzer 2022; Maggiori 2023).

curaatheid – maar ook te kwalificeren.[5] Het gaat in het kader van dit boek dan vooral om de effecten van (het optreden op basis van) valspositieven op het leven van burgers.[6] Sinds de internationale opkomst van voorspellende algoritmen in het politiewerk zijn er vooral zorgen over hoe deze effecten van het gebruik van (deze) algoritmen over de verschillende groepen burgers in de samenleving zijn verdeeld. In verschillende studies en beschouwingen is geconcludeerd dat burgers met een migratieachtergrond onevenredig veel te maken krijgen met deze (negatieve) effecten.[7] Kortom: algoritmen kunnen leiden tot ongelijke behandeling, tot discriminatie.

Om deze effecten van het gebruik van risicotaxerende algoritmen in het politiewerk te begrijpen, is het van belang in te gaan op zowel de accuraatheid van algoritmen als de effecten van het optreden op basis van deze algoritmen. Hierna ga ik op beide in. In de uitwerking gebruik ik diverse vormen van predictive policing als voorbeeld waarbij de nadruk ligt op risicotaxatie op persoonsniveau. De reden hiervoor is dat deze algoritmen het meeste risico geven op discriminerende effecten.[8]

Vertekening in uitkomsten van algoritmen

Zoals gezegd: risicotaxerende algoritmen leiden altijd tot valspositieven en valsnegatieven. Dit komt omdat er sprake is van *bias*: vertekening. Er kan onderscheid worden gemaakt tussen verschillende 'lagen' van vertekening.[9] De *basis-laag* van vertekening is onlosmakelijk verbonden met de praktijk van risicotaxatie.[10] Bij risicotaxatie op persoonsniveau (predictive identification) worden data over de groep gebruikt om uitspraken te doen over het individu. Ten aanzien van data over de groep kan worden gedacht aan factoren als geslacht en leeftijd. Wanneer dergelijke factoren worden opgenomen in algoritmen om iemands gedrag te voorspellen, worden veronderstelde groepskenmerken – bijvoorbeeld: mannen zijn oververtegenwoordigd in criminaliteit – gebruikt om op individueel niveau tot een risicotaxatie te komen. Anders gezegd: mensen worden niet meer als individuen, maar als leden van een algoritmisch samengestelde risicogroep aangemerkt.[11] Dit leidt per definitie tot een vorm van bias, omdat een groepskenmerk nooit determinerend is voor individueel gedrag. Of anders gezegd: het is in letterlijk zin per definitie discrimineren, want meer risicovolle burgers worden van minder risicovolle burgers onderscheiden op basis van kenmerken van groepen individuen die de betreffende burger voor een deel niet kan beïnvloeden.[12] Dit heeft dus niets te maken met de komst van AI, maar was altijd al een fundamentele vorm van

5 Maggiori 2023.
6 Brayne 2021.
7 Zie onder andere Amnesty International 2020; Brayne 2021; Ferguson 2017a; Hamilton 2021; O'Neil 2016; Shapiro 2020.
8 Zie ook Egbert & Leese 2021.
9 Eckhouse et al. 2019.
10 Zie ook Harcourt 2007.
11 Schermer & Galič 2023.
12 Zie ook Bijlsma, Bex & Meynen 2019; De Vries et al. 2021.

vertekening in alle pogingen om het gedrag van burgers te voorspellen op basis van groepskenmerken.

> *'This is a characteristic that various AI systems share with traditional police approaches: the propensity to stereotype. Inferences are drawn about a person because of one or more shared interests or attributes, irrespective of their more complex life experiences, personalities and hopes for the future.'*[13]

Het fundamentele karakter van de vertekening maakt dat het een basis-laag is. Op het moment dat ervoor wordt gekozen om dergelijke variabelen op te nemen in een algoritme is er per definitie van deze vertekening sprake. Deze vertekening kan uiteindelijk leiden tot verschil in behandeling tussen burgers dat niet kan worden gerechtvaardigd. Om die reden benadrukt Amnesty International in het rapport over de sensing proeftuin in Roermond (zie hoofdstuk 17) dat dit in strijd is met het internationale raamwerk op het gebied van mensenrechten. 'In any case, differential treatment based on alleged overrepresentation of certain groups is not in line with the international human rights framework.'[14] Men zegt dus: op het moment dat je ervoor kiest om dergelijke groepskenmerken – via algoritmen – te gebruiken voor de behandeling/het optreden op individueel niveau, dan doe je eigenlijk al iets dat niet strookt met bescherming van mensenrechten.

De *tweede laag* van vertekening heeft te maken met de *data* die worden gebruikt. Ik beperk me hier tot data over criminaliteit. In een ideale wereld heeft de data die in AI-politiesystemen worden gebruikt betrekking op de werkelijke criminaliteit. Dit is echter niet het geval, omdat de werkelijke criminaliteit niet kan worden gemeten.[15] Er worden allerlei proxy's voor gebruikt, die een vertekening zijn van de werkelijke criminaliteit.[16] In geval van brengdelicten gaat het om meldingen en (vooral) aangiften van burgers. Ten aanzien van haaldelicten gaat het onder andere om aanhoudingen. Burgers doen niet van alle criminaliteit aangifte of melding en de politie is selectief in waar zij naar op zoek gaat. En al gaat zij op zoek naar criminaliteit, er wordt ook heel veel niet gevonden. In de criminologie wordt dit ook wel het *dark number* genoemd: de criminaliteit die niet is geregistreerd. Van deze criminaliteit is dus geen data en die data kunnen dus ook niet worden gebruikt in AI-systemen.[17] Niet als trainingsdata voor de ontwikkeling van de algoritmen, maar ook niet als feedback om algoritmen te laten leren van hun omgeving. Het laatste is dus ook van belang: de feedback is altijd partieel.[18]

13 McDaniel & Pease 2021b: 86.
14 Amnesty International 2020: 39.
15 Hamilton 2021.
16 Dit punt kan nog wat breder worden gemaakt: er is een verschil tussen de data die idealiter worden gebruikt en die beschikbaar zijn. In de praktijk moet worden gewerkt met data die beschikbaar zijn en dit heeft gevolgen voor onder andere de ontwikkeling van algoritmen (zie ook Mutsaers & Van Nuenen 2023).
17 Egbert & Leese 2021.
18 Ensign et al. 2018.

Met betrekking tot de data die wel worden gebruikt, is het essentieel om – in het licht van het voorgaande – onderscheid te maken tussen data die door de politie worden geproduceerd en data die door burgers worden geproduceerd.[19] Tussen beide doen zich verschillen in vertekening voor.[20] Data die door de politie worden geproduceerd – data *van* de politie – bevatten vertekening als gevolg van de keuzes die in de politieorganisatie worden gemaakt ten aanzien van wat (thema, plaatsen, personen, et cetera) meer en minder aandacht krijgt en hoe situaties worden afgehandeld (bijvoorbeeld wel of niet aanhouden). Deze keuzes werken door in de data. Data die door burgers worden geproduceerd – data *voor* de politie – bevatten vertekening als gevolg van de keuzes die burgers maken met betrekking tot het melden en aangeven van criminaliteit. Vooral de vertekening in de data *van* de politie is problematisch, omdat deze vertekening (deels) wordt veroorzaakt door prioriteiten, vooroordelen en andere eenzijdigheden binnen de politieorganisatie en de bredere institutionele omgeving.[21] Wanneer deze data worden gebruikt om criminaliteit te voorspellen, dan worden deze eenzijdigheden meegenomen (gereproduceerd) in de uitkomsten van algoritmen.

Het bovenstaande leidt ertoe dat systemen van predictive identification met betrekking tot vertekende data problematischer zijn dan systemen van predictive mapping.[22] Systemen van predictive mapping – zoals het CAS in Nederland (zie hoofdstuk 19) – gebruiken (veelal) data voor de politie, aangevuld met bevolkingsdata. Systemen van predictive identification gebruiken (veelal) ook data van de politie die betrekking hebben op individuen: persoonsgegevens. Bij data over individuen moet onder andere rekening worden gehouden met de oververtegenwoordiging van burgers – vooral jongeren – met een migratieachtergrond in het justitiële systeem. Onderzoek naar deze oververtegenwoordiging suggereert dat de verdenkingskans – de kans dat hetzelfde criminele gedrag leidt tot een verdachtenregistratie – voor jongeren met een migratieachtergrond twee tot drie keer zo groot is dan voor jongeren met een Nederlandse

19 Ik ga hier in op een beperkt aantal databronnen. Zie Wessels (2023) voor een uitgebreider overzicht van typen data die worden gebruikt voor *algorithmic policing*.

20 Brayne 2021.

21 Ferguson 2017a.

22 Dit wil niet zeggen dat systemen van predictive mapping niet problematisch kunnen zijn (zie ook Mutsaers & Van Nuenen, 2023). Ook systemen van predictive mapping zijn gevoelig voor discriminerende uitkomsten. Dit wordt veroorzaakt door er in het algoritme diverse datapunten worden gebruikt die correleren met de sociaal-economische status van wijken en de burgers die er wonen, zoals het inkomensniveau (Ferguson, 2017a; Oosterloo & Van Schie, 2018). Het algoritme dirigeert de politie al snel naar buurten waar burgers met een 'lage' sociaal-economische status wonen. Deze buurten kunnen te maken krijgen met *overpolicing* of *spatial stigmatization* (Završnik, 2018). Daarnaast komt uit onderzoek naar voren dat plaatsgebonden risicotaxaties kunnen doorwerken in persoonsgebonden risicotaxaties (Egbert & Leese, 2021). Dit wil zeggen dat politieagenten in buurten die zijn aangemerkt als 'hoog risico' extra wantrouwend zijn naar burgers die zij op straat tegenkomen en dus snel iemand verdacht vinden en kunnen overgaan tot proactieve controles. Zie ook het rapport van de Algemene Rekenkamer (2022) waarin onder andere het CAS is getoetst aan de hand van een toetsingskader. De conclusie die op basis hiervan is getrokken, is dat het CAS op alle aspecten van het toetsingskader niet voldoet. Dit betreft onder andere controle op de juistheid van gegevens en *controle op bias*. Men heeft niet vastgesteld dat het CAS leidt tot discriminerende uitkomsten, maar constateert wel dat er door de politie onvoldoende maatregelen zijn genomen om dit te voorkomen. De Algemene Rekenmaker kan dus niet uitsluiten dat er bij het CAS een onwenselijke systematische afwijking voor specifieke personen of groepen is ontstaan.

achtergrond.[23] Dergelijke vertekende data leiden ertoe dat burgers met een migratieachtergrond sneller als risicovol worden aangemerkt, terwijl burgers met een Nederlandse achtergrond juist onderdeel zijn van valsnegatieven: zij krijgen lage(re) risicoscores, terwijl in werkelijkheid een hogere score gerechtvaardigd is. Kortom: burgers met een Nederlandse achtergrond hebben een grotere kans om onterecht met rust te worden gelaten.[24]

Dan naar de *derde laag* van vertekening: de (modellering van de) algoritmen zelf. In hoofdstuk 24 is het al aan de orde gekomen: datagedreven politiewerk leidt niet tot het verdwijnen van de discretionaire ruimte, maar tot het verplaatsen van aspecten ervan naar het moment waarop keuzes in het ontwerp van algoritmen worden gemaakt. De keuzes die in het ontwerp van algoritmen kunnen worden gemaakt, variëren naargelang het type algoritme. Het aantal keuzes is in de regel groter wanneer het algoritme regelgebaseerd is, omdat in dat geval de variabelen en het gewicht van die variabelen volledig door mensen worden bepaald.[25] Bij zelflerende algoritmen zijn er echter ook allerlei keuzes aan de orde, zoals de trainingsdata die worden geselecteerd,[26] de feedbackdata die worden gebruikt[27] en de aanpassingen die aan het zich ontwikkelde algoritme worden gedaan.[28] Deze keuzes in zowel regelgebaseerde als zelflerende algoritmen hebben consequenties voor hoe algoritmen werken en dus op hoe algoritmische besluitvorming plaatsvindt. Algoritmen zijn dus niet neutraal, want aan de keuzes van mensen liggen waarden en betekenissen ten grondslag.[29] In dat opzicht zijn datawe-

23 Bezemer & Leerkes 2021.

24 In het verlengde van 'onterecht met rust laten' is het van belang om een aanvullende vraag te stellen: over welke vormen van criminaliteit gaan deze systemen eigenlijk? Dit betreft altijd vormen van criminaliteit waarover data beschikbaar zijn die het mogelijk maken om tot voorspellingen te komen, bijvoorbeeld bepaalde geweldsdelicten. Het gaat dus om bepaalde delicten en de kenmerken van de individuen die correleren met deze delicten (Završnik, 2018). Hierbij kan worden gedacht aan opleidingsniveau, inkomensniveau en dergelijke. Er worden dus allerlei kenmerken gebruikt die betrekking hebben op of correleren met de sociaal-economische status van een persoon (zie Ferguson, 2017a). In het gehele strafrechtelijke systeem – van risicokinderen tot veroordeelden – ligt er onvermijdelijk een nadruk op burgers die in kwetsbare wijken wonen met een laag opleidingsniveau en relatief weinig inkomen. Uit de data over de betreffende gedragingen/delicten komt immers naar voren dat dit de factoren zijn die met deze gedragingen correleren. De beperking is echter dat deze data per definitie eenzijdig zijn, omdat ze een weerslag zijn van onder andere de beleidsprioriteiten en inspanningen van de politie en andere instanties als gevolg van die beleidsprioriteiten. Anders geformuleerd: waar zijn de risicotaxatie instrumenten van milieucriminaliteit en 'witteboordencriminaliteit' (zie ook O'Neil, 2016)? Die zijn er (bij mijn weten) niet, omdat er minder nadruk op ligt (en er in de regel niemand aangifte van doet) en daardoor ook minder data over zijn. Deze eenzijdigheid werkt door in de delicten waarvoor predictive identification beschikbaar is en de risicoburgers die via deze delicten (niet) in beeld komen.

25 Hamilton 2021.

26 Een algoritme dat is ontwikkeld op basis van vertekende trainingsdata creëert geen bias, maar reflecteert een bias die al aanwezig is. Zie hiervoor onder andere: Berk 2021; Bijlsma et al. 2019; Lin 2022.

27 Het maakt uit welke feedback aan de software wordt gegeven. Neem de proeftuin in Roermond: wanneer wordt iets gedefinieerd als een onterechte 'hit'? Als de definitie van een 'hit' ruim wordt genomen – er wordt bijvoorbeeld niets aangetroffen bij een proactieve controle, maar politiemensen die controleren hebben wel het gevoel dat er iets niet klopt en beschouwen het daarom als een terechte hit (en registreren het als zodanig) – dan leert het systeem te weinig van valspositieven. Zie ook: McDaniel & Pease 2021b.

28 McDaniel & Pease 2021b.

29 Adensamer & Klausner 2021; Brayne 2021; Hamilton 2021; McDaniel & Pease 2021b; O'Neil 2016.

tenschappers en AI-softwareontwikkelaars te beschouwen als beleidsmakers.[30] Marc Schuilenburg wijst op het risico dat deze functionarissen – vanuit hun eigen geprivilegieerde positie (*coding elite*) – handelen zonder oog voor het gegeven dat hun eigen beslissingen kunnen bijdragen aan discriminatoire praktijken.[31]
Het ontwerp van algoritmen kan in het bijzonder (maar zeker niet alleen) leiden tot discriminerende uitkomsten wanneer in het algoritme etniciteit of een proxy daarvoor is opgenomen. Hierop wijst Amnesty International in geval van de proeftuin in Roermond, aangezien in het algoritme het land van herkomst van het voertuig als kenmerk was opgenomen (volgens Amnesty is dit een proxy voor etniciteit).[32] Bij drie landen leidt dit – in combinatie met andere kenmerken – tot een hogere risicoscore. Amnesty International benadrukt dat dit in strijd is met het discriminatieverbod.

Rechtszaak etnisch profileren door de Koninklijke Marechaussee[33]
Op 14 februari 2023 diende bij de rechtbank in Den Haag het hoger beroep in de rechtszaak omtrent etnisch profileren door de Koninklijke Marechaussee (KMar). Deze zaak draait om het onderdeel van de KMar dat is belast met het mobiel toezicht en in dat kader controles uitvoert aan de Nederlandse grens. Hierbij kunnen personen die net de grens zijn gepasseerd, worden staande gehouden en worden gevraagd naar hun identiteit, nationale identiteit en verblijfsrechtelijke positie. De KMar selecteert de personen die zij aan een dergelijke controle onderwerpt aan de hand van risicoprofielen. In bepaalde gevallen worden hierbij ook persoonlijkheidskenmerken gebruikt die zijn gebaseerd op ras of etniciteit (in combinatie met andere indicatoren). Twee personen die op deze wijze zijn geselecteerd en gecontroleerd, hebben in samenwerking met maatschappelijke organisaties de rechter gevorderd om aan de Staat een verbod op te leggen om nog langer aan ras ontleende kenmerken te gebruiken bij de selectie van personen in het kader van deze controles. De handelswijze van de KMar is volgens hen in strijd met diverse mensenrechtenverdragen. De rechtbank heeft in eerste aanleg de KMar in het gelijk gesteld. Volgens de rechtbank mag etniciteit *onderdeel zijn* van risicoprofielen en kan iemands huidskleur een objectieve aanwijzing zijn voor iemands vermeende nationaliteit. In hoger beroep hebben de appelanten alsnog gelijk gekregen. Het hof is van oordeel dat de KMar onderscheid maakt op grond van ras of etniciteit. Dit heeft ernstige gevolgen en mag alleen worden gemaakt als daar bijzonder zwaarwegende redenen voor zijn. Deze redenen zijn door de Staat niet aangetoond. Dit impliceert dat de KMar zich schuldig maakt aan discriminatie op grond van

30 Lin 2022.
31 Zie o.a. https://www.websitevoordepolitie.nl/oratie-marc-schuilenburg-making-surveillance-public/ (voor het laatst geraadpleegd op 11 augustus 2023).
32 Amnesty International 2020.
33 Gebaseerd op https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:GHDHA:2023:173 (voor het laatst geraadpleegd op 21 februari 2023).

ras en dat is verboden. Het hof heeft de Staat verboden om bij de uitvoering van de mobiele toezichts- en veiligheidscontroles selectiebeslissingen te nemen die (mede) zijn gebaseerd op ras. De toevoeging 'mede' is van belang: waar de rechtbank eerder oordeelde dat etniciteit een van de indicatoren mag zijn, oordeelt het hof anders. Het hof maakt hierbij gebruik van criteria van het EHRM. Dit wil zeggen dat er sprake is van verboden discriminatie als 'het aan ras of etniciteit ontleende kenmerk in zoverre beslissend is, dat de desbetreffende persoon niet voor controle zou zijn geselecteerd indien, bij gelijkblijvende overige omstandigheden, dat kenmerk er niet was geweest'. Hier is volgens het hof dus sprake van. De Staat heeft volgens het hof tevens niet aangetoond dat ras of etniciteit geschikt is om nationaliteit of herkomst vast te stellen (of in te schatten). Dit is expliciet een erkenning van multicultureel, veelkleurig Nederland waarin huidskleur niets zegt over nationaliteit.[34] De uitspraak van het hof heeft betrekking op de betreffende controles door de KMar, maar kan ook gevolgen hebben voor de politie. De politie bestudeert de gevolgen van de uitspraak en gaat werkwijzen – waar nodig – aanpassen.[35] Hierop vooruitlopend kan worden geconcludeerd dat formele risicoprofielen waarin etniciteit of ras – dan wel een daaraan ontleend kenmerk – zijn opgenomen niet (meer) kunnen worden gebruikt.[36] Dit wil zeggen dat deze indicatoren geen onderdeel mogen zijn van algoritmen. De discussie zal vooral gaan over wat aan etniciteit of ras ontleende kenmerken zijn.

Het is van belang te benadrukken dat de wijze waarop algoritmen worden ontworpen niet alleen kan bijdragen aan discriminatie van burgers met een migratieachtergrond, maar in potentie ook aan het reduceren van deze discriminatie.[37] In het ontwerp van zelflerende algoritmen kunnen – gegeven de vertekening in data – diverse compenserende maatregelen worden genomen die ertoe leiden dat delen van de populatie anders worden behandeld met het oog op meer rechtvaardigheid.[38] Hiermee wordt de kans op valpositieven in dit deel van de populatie verkleind.[39] Er is in de (data)wetenschap echter veel discussie over de verschillende methoden om meer rechtvaardigheid te realiseren en er is vooralsnog weinig inzicht in hoe deze manieren of methoden bijdra-

34 https://www.nrc.nl/nieuws/2023/02/15/uit-de-rij-gehaald-worden-mag-nog-steeds-maar-ras-mag-daarbij-nooit-beslissend-zijn (voor het laatst geraadpleegd op 21 februari 2023).

35 https://www.politie.nl/nieuws/2023/februari/16/00-politie-leert-van-uitspraak-etnisch-profileren-kmar.html (voor het laatst geraadpleegd op 21 februari 2023).

36 Het oorspronkelijke ontwerp van het algoritme van het RTI-Geweld is bijvoorbeeld niet meer toegestaan (zie hiervoor hoofdstuk 19).

37 Ávila, Hannah-Moffat & Maurutto 2021.

38 Bijvoorbeeld: een zelflerend algoritme voor predictive identification kan worden ingesteld op een manier die relatief veel valsnegatieven oplevert, omdat het voorkomen van burgers die onterecht als hoog risico worden aangemerkt belangrijker wordt gevonden dan het voorkomen van burgers die onterecht als laag risico worden aangemerkt. Dit gaat over de balans tussen precision (rechtvaardigheid) en recall (veiligheid van de maatschappij). Zie: Bijlsma, Bex & Meynen 2019; Bland 2020.

39 Zie ook Bijlsma, Bex & Meynen 2019; Bland 2020.

gen aan het daadwerkelijk reduceren van (de kans op) discriminatie.[40] Anders gezegd: de discussie is nog niet beslecht. Een onderliggend probleem hierbij is dat rechtvaardigheid een abstract, ethisch concept is[41] en geen statistisch concept: rechtvaardigheid is lastig te berekenen.[42] Het hanteren van de ene of de andere methode voor het bevorderen van rechtvaardigheid (*fairness metrics*) is daarmee een normatieve keuze, die samenhangt met een opvatting over wat eerlijk is.[43]

In het kader van de accuraatheid en rechtvaardigheid van algoritmen is het tot slot van belang om stil te staan bij de beoordeling van hun onvermijdelijke imperfectie (zie ook hoofdstuk 26). Anders gezegd: het voorgaande maakt duidelijk dat er het nodige is aan te merken op hoe risicotaxerende algoritmen in het algemeen en in het politiewerk in het bijzonder functioneren. De vraag is echter welke betekenis hieraan moet worden gegeven. Risicotaxatie in het politiewerk is in essentie niet nieuw en voor valspositieven geldt hetzelfde.[44] Toen ik ruim acht jaar geleden onderzoek verrichtte naar proactief controleren, taxeerden politieagenten in feite ook risico's – men maakte inschattingen op basis van informele profielen[45] – die discriminerende uitkomsten hadden.[46] En lang daarvoor ook al. Kortom: 'Humans were running such probabilistic assessments in their minds long before cops used computers.'[47] Dus hoe moeten we het functioneren van algoritmen beoordelen: in het licht van het ideaal van volledige accuraatheid of in het licht van de huidige praktijk? De huidige praktijk lijkt het meest logische en 'eerlijke' referentiepunt, want het streven is immers die te verbeteren.

> '*… the baseline for forecasting accuracy is current practice, not perfection. The guiding question is whether predictive policing leads to improvements in accuracy beyond current procedures. There have been some successes, but so far we have no general conclusions one way of the other.*'[48]

De laatste zin in bovenstaand citaat is van belang en is in het hoofdstuk over effectiviteit ook al aan de orde gekomen: we kunnen nog geen stevige uitspraken doen over of de huidige AI-systemen veel accurater zijn dan mensen of regelgebaseerde algoritmen. Er zijn redenen om aan te nemen van wel, maar een stevige empirische basis voor het

40 Ávila, Hannah-Moffat & Maurutto 2021; Dressel 2017.
41 Zie Manning 2010 over rechtvaardigheid en politiewerk.
42 Ávila, Hannah-Moffat & Maurutto 2021.
43 Rathenau Instituut 2023.
44 Zie ook Niculescu-Dincă 2016.
45 Het gebruik van een algoritme voor proactieve controles – zoals in de sensing proeftuin Roermond – is in feite een vorm van formeel profileren. In geval van een modelgedreven algoritme kan het profiel worden geëxpliciteerd. Dit is in potentie doorzichtiger dan informeel profileren (zie ook Prins, 2020). Deze transparantie is bij datagedreven, zelflerende algoritmen door de bank genomen problematischer (zie ook hoofdstuk 29).
46 Landman & Kleijer-Kool 2016.
47 Brayne 2021: 123.
48 Berk 2021: 224.

doen van uitspraken ontbreekt vooralsnog.[49] Duidelijk is in ieder geval wel dat algoritmische risicotaxatie vooralsnog niet vrij is van vertekening en dat deze vertekening niet het gevolg is van het gebruik van algoritmen, maar van de data die door mensen worden geproduceerd en de keuzes die in het ontwerp en gebruik van algoritmen worden gemaakt.

> *'In other words, algorithmic bias is just a symptom. The root cause of bias in AI is us. Our biases and the institutions we've constructed – laws, police, justice – reproduce the problems we are seeing in our technology. We cannot overlook the human element of this issue. People design AI. People use AI. Most importantly, people choose how AI is used on other people.'*[50]

Er is echter wel een belangrijk verschil tussen de vertekening of bias in menselijke risicotaxatie en die in algoritmische risicotaxatie. Dit verschil hangt samen met het gebruik: algoritmische risicotaxatie leidt tot schaalvergroting. De bias in algoritmische besluitvorming kan op veel meer gevallen worden toegepast. Deze schaalvergroting zorgt voor een toename van het aantal valspositieven en daarmee voor het risico op een absolute toename van gevallen van ongelijke behandeling.[51] Aangezien het – zoals gezegd – zeer aannemelijk is dat valspositieven vooral betrekking hebben op burgers in kwetsbare omstandigheden, is een toename van het aantal valspositieven vooral nadelig voor hen.

Effecten van het (proactieve) optreden

Met het woord 'nadelig' in de voorgaande zin zijn we aanbeland bij het tweede, kortere deel van dit hoofdstuk. In het kader van het risico op discriminatie bij algoritmische risicotaxatie is het essentieel om voorbij de uitkomsten van algoritmen te gaan. Het gaat er uiteindelijk om hoe de uitkomsten van algoritmen worden geduid en worden gebruikt in het politiewerk.[52] Discriminatie ontstaat als uitkomsten van algoritmische risicotaxatie in opsporings- en handhavingspraktijken worden gebruikt en leiden tot ongelijke behandeling van burgers. In de politiepraktijk bestaat deze ongelijke behandeling vooral uit meer intensieve surveillance en controle.[53] De effecten hiervan zijn bij systemen op het gebied van predictive identification in potentie schadelijker dan in geval van systemen op het gebied van predictive mapping.[54] Simpel geformuleerd: een

49 Algoritmische risicotaxatie wekt wel de schijn van accuratere uitkomsten, veelal gedefinieerd in termen van objectiviteit. Deze objectiviteit is een argument in het publieke debat over het gebruik van algoritmen: vooral in de VS zijn AI-systemen door de politie geïntroduceerd met de belofte van meer objectiviteit en neutraliteit (zie onder andere Brayne, 2021; Ferguson, 2017a), maar ook in Nederland worden dergelijke argumenten weleens gebruikt, onder ander bij de sensing proeftuin in Roermond (zie Prins, 2020). Deze schijn van objectiviteit kan tevens een rol spelen bij het gebruik in de praktijk: de uitkomsten van algoritmen worden dan door politiemensen als 'waar' beschouwd en worden kritiekloos overgenomen (zie Niculescu-Dincă, 2016).

50 Lin 2022: 42.

51 Brayne 2021; Lin 2022.

52 Zie ook Waardenburg, Sergeeva & Huysman 2020.

53 Niculescu-Dincă 2016.

54 Degeling & Berendt 2018.

politie die disproportioneel, en zonder redelijke en objectieve rechtvaardiging,[55] vaker surveilleert in de ene buurt dan in de andere buurt is naar mijn indruk minder schadelijk dan een politie die bepaalde personen 'onterecht' als een hoog risico aanmerkt en op basis hiervan repressief optreedt.

Khalid van de Van Wougroep[56]

In een onderzoek naar de integrale aanpak van een jeugdgroep – genaamd de Van Wougroep – uit de Amsterdamse Diamantbuurt komen de nadelige gevolgen die een risicoburger kan ondervinden duidelijk aan het licht. De aanpak van de Van Wougroep werd gekenmerkt door het onderscheid tussen de rode groep (gedefinieerd als de 'criminele harde kern'), de gele groep (gedefinieerd als 'voornamelijk crimineel, deels overlastgevend') en de groene groep (gedefinieerd als 'voornamelijk overlastgevend'). Het onderscheid in deze doelgroep was bepalend voor de aanpak: van zeer repressief (rood) naar 'zorg op maat' (groen). Khalid was – ondanks het ontbreken van antecedenten – een van de jongeren in de rode groep. Dit had onder andere als gevolg dat hij aan de lopende band werd staande gehouden en bekeurd door de politie en er veel mutaties over hem in het politiesysteem terechtkwamen. Sommige politieagenten vertelden hem dat ze er alles aan zouden doen om hem 'in de bak te krijgen'. Khalid komt ook op de Top 600 – een lijst van 600 personen in de regio Amsterdam-Amstelland die in de afgelopen jaren relatief veel high impact delicten hebben gepleegd – terecht, al kon niemand hem vertellen wat hier de reden voor is. Het lukt met behulp van een advocaat om van de lijst te komen. Ten tijde van de integrale aanpak voelt Khalid zich geregeld depressief en onzeker. In het onderzoek naar de jeugdgroep geven een straathoekwerker en een vertegenwoordiger van het stadsdeel aan dat Khalid onterecht in de hoogste risicogroep terecht is gekomen. Volgens Khalid heeft hij aan zijn ouders te danken dat hij niet daadwerkelijk de criminaliteit ingaat, onder andere omdat zij de boetes betalen en hij geen schulden krijgt. Hij werkt op dit moment als leidinggevende in de detailhandel.

Bovenstaand voorbeeld maakt duidelijk dat burgers die onterecht in een hoge risicogroep worden geplaatst hier veel nadelige gevolgen van kunnen ondervinden.[57] Eenzijdigheid in surveillance door de politie kan gemakkelijk leiden tot effecten die de

55 Een oordeel over de redelijke en objectieve rechtvaardiging is vanwege het dark number overigens lastig te geven.

56 Gebaseerd op: Peeters & Van Dongen 2022.

57 Zie ook deze documentaire waarin moeders wiens zonen op de Top400 staan aan het woord komen: https://www.2doc.nl/documentaires/2022/11/moeders.html (voor het laatst geraadpleegd op 8 januari 2023). Zie ook Jansen (2022) over de Top400. In de Top400 is gebruikgemaakt van ProKid (zie hoofdstuk 19). Tot slot: zie dit artikel in *Follow the Money* over het gebruik van het RTI-Geweld en de casus van 'Jay': www.ftm.nl/artikelen/nederlandse-politie-gebruikt-minority-report-algoritme (voor het laatst geraadpleegd op 25 augustus 2023).

politie bevestigen in diens gelijk. Hierbij kan onder andere worden gedacht aan vijandigheid in interactie tussen politie en de betreffende burgers, mutaties van verdacht gedrag in systemen of het constateren van overlast en/of strafbare feiten.[58] Er treedt dan dus een selffulfilling prophecy op. Niculescu-Dincă komt op basis van onderzoek naar technologiegebruik door de politie in onder andere Nederland tot de volgende conclusie:

> *'… labels in police systems concerning 'problematic', 'suspected' or 'risk' entities are not only necessary but often also sufficient justifications for proactive surveillance practices. What we have seen though is that, in their turn, surveillance increases the chance for encountering problematic situations with people in these categories (compared to other categories). Entering a cycle of suspicion-surveillance solidifies incentives for intervention and makes it difficult for the enacted entities to invalidate the reasons for which they raised police interest.'*[59]

Het is van belang te benadrukken dat deze mechanismen effecten hebben die het individu ruimschoots overstijgen. Het gaat om bevolkingsgroepen die via de wijken waar zij wonen of de lijsten waarop zij als individu staan disproportioneel worden onderworpen aan sociale controle en repressief optreden door de politie.[60] Deze 'sortering' – de (geautomatiseerde) systematische ongelijke behandeling van bepaalde groepen in de samenleving – heeft de neiging om in de tijd toe te nemen, omdat de opbrengsten van disproportionele sociale controle veelal aanleiding zijn voor meer disproportionele sociale controle.

> *'Marginalized groups face higher levels of data collection when they access public benefits, walk to highly policed neighborhoods, enter the health-care system, or cross national borders. The data acts to reinforce their marginality when it used to target them for suspicion and extra scrutiny.'*[61]

Dit zelfversterkende effect leidt op termijn tot substantiële verschillen in het politieoptreden tussen bevolkingsgroepen en uiteindelijk ook tot substantiële verschillen in de uitkomsten van het strafrechtelijke systeem, die zich niet meer verhouden tot de (eventuele) verschillen in crimineel gedrag tussen deze bevolkingsgroepen. Wie benieuwd is naar wat de gevolgen hiervan op een samenleving zijn, kan het best naar de VS kijken waar zwarte burgers structureel en op uiteenlopende manieren worden benadeeld door de wijze waarop het strafrechtelijke systeem wordt gericht en functioneert.[62] De sociale kosten van deze uitsluitingsmechanismen zijn hoog. Naar mijn indruk is de

58 Harcourt (2007) wijst erop dat wie binnen bepaalde bevolkingsgroepen op zoek gaat naar criminaliteit altijd wel wat zal vinden. Zie ook Landman & Kleier-Kool 2016.
59 Niculescu-Dincă 2016: 138.
60 Zie ook Schermer & Galič 2023.
61 Eubanks 2018: 6.
62 Zie hiervoor onder andere Harcourt 2007.

mate van disproportionaliteit in het politieoptreden in Nederland niet vergelijkbaar met die in de VS, maar het is – mede gegeven de schaalvergroting als gevolg van technologie – wel een risico waarmee we in toenemende mate rekening moeten houden. De toeslagenaffaire heeft daarnaast laten zien dat deze mechanismen zich – weliswaar in een ander domein – ook in Nederland voordoen.

Toeslagenaffaire[63]

De toeslagenaffaire draait om de aanpak van fraude bij de kinderopvangtoeslag.[64] Hierbij werd een risicoclassificatiemodel – een beslisboom[65] – ingezet dat onder andere tot doel had om oneigenlijk gebruik van toeslagen te voorkomen.[66] Dit model werd door de afdeling Toeslagen van de Belastingdienst gebruikt om te selecteren welke nieuwe aanvragen of wijzigingen in bestaande aanvragen voor handmatige behandeling in aanmerking moesten komen. Dit waren de aanvragen die werden geclassificeerd als hoog risico. In de fase van handmatige behandeling werd uitgegaan van een strikte toepassing van wet- en regelgeving. Wanneer werd geconstateerd dat bepaalde informatie in de aanvraag ontbrak of een klein deel van de eigen bijdrage niet was betaald, kon een medewerker de toeslag stopzetten en terugvorderen. In het model werden uiteenlopende indicatoren gebruikt, waaronder het al dan niet hebben van een Nederlandse nationaliteit en de 'leeftijd' van het burgerservicenummer. Door gebruik van deze indicatoren hadden burgers met een niet-Nederlandse nationaliteit of recente Nederlandse nationaliteit (dubbele nationaliteit) een grotere kans op handmatige beoordeling en daarmee ook op repressieve maatregelen.[67] Deze repressieve maatregelen hebben bij een deel van de betreffende burgers geleid tot schulden en allerlei aanpalende problemen. De AP concludeerde op basis van onderzoek dat de gebruikte algoritmen hebben geleid tot permanente, structurele en onnodige (negatieve) aandacht voor nationaliteit binnen de aanpak van fraude.[68] Amnesty International concludeerde dat de algoritmen hebben geleid tot etnisch profileren.[69]

De toeslagenaffaire is het meest pijnlijke voorbeeld van de gevolgen die optreden op basis van algoritmische risicotaxatie voor (kwetsbare) burgers kunnen hebben. De toe-

63 Deze beschrijving is gebaseerd op Tweede Kamer der Staten-Generaal 2020.
64 Zie Verhoeven 2023 voor meer historie en context bij de toeslagenaffaire.
65 Het was – voor zover ik heb kunnen nagaan – geen zelflerend algoritme en daarmee geen 'moderne' AI (zie hoofdstuk 5).
66 Dit model werd ook ingezet voor de huurtoeslag, maar ik beperk me hier tot de kinderopvangtoeslag.
67 Twee opmerkingen zijn van belang. In een dergelijk risicoclassificatiemodel gaat het altijd om scores op meerdere factoren die een bepaald gewicht hebben in de risicoclassificatie. Daarnaast: in de populatie die handmatig werd beoordeeld was niet alleen sprake van een oververtegenwoordiging van burgers met een niet Nederlandse nationaliteit, maar ook van burgers die alleenstaand zijn en/of een laag inkomen hebben.
68 AP 2020.
69 Amnesty International 2021.

slagenaffaire heeft echter nog iets anders laten zien.[70] Individuele, als (hoog) risico getaxeerde, burgers hebben door de bank genomen weinig mogelijkheden om iets aan de risicotaxatie en het daarop gebaseerde optreden van uitvoeringsorganisaties te doen.[71] Dit heeft onder andere te maken met de toenemende macht waarover uitvoeringsinstanties in het tijdperk van AI beschikken. Het evenwicht der machten raakt hierdoor verstoord. Hierover gaat het volgende hoofdstuk.

70 De toeslagenaffaire wordt hier als voorbeeld gebruikt. Het probleem dat hierna wordt behandeld, doet zich ook in de context van het politiewerk voor. De casus van Khalid is hier een illustratie van, maar zie ook het eerder aangehaalde artikel van *Follow the Money* over het RTI-Geweld.

71 Zie ook Rathenau Instituut 2023.

29 Evenwicht der machten

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*.[1] Deze scheiding is voor de rechtsstaat essentieel, omdat deze – bij adequaat functioneren in de praktijk – zorgt voor machtsbalans en het voorkomen van machtsmisbruik. Datagedreven politiewerk kan afbreuk doen aan de effectiviteit van het evenwicht der machten (checks-and-balances). In dit hoofdstuk licht ik dit risico toe.[2]

De macht van de uitvoering

De opkomst van het gebruik van (zelflerende) algoritmen in het politiewerk heeft zich in belangrijke mate afgespeeld buiten het gezichtsveld van de politiek. Marc Schuilenburg noemde het vijf jaar geleden een 'stille technologische revolutie' waarover in beperkte mate politiek-maatschappelijk debat plaatsvindt.[3] Dit wil onder andere zeggen dat over de ontwikkeling en inzet van algoritmische systemen geen politieke discussie plaatsvindt. Zo heeft de AP erop gewezen dat de (landelijke) inzet van het CAS is benaderd als een uitvoeringskwestie waarover geen of beperkt verantwoording is afgelegd.[4] Bits of Freedom heeft een vergelijkbare (kritische) opmerking gemaakt over de inzet van CATCH: er is geen voorstel langs de Tweede Kamer gegaan.[5] Deze 'stille revolutie' is een internationaal patroon. De commissie voor justitie en binnenlandse zaken van de House of Lords in het VK publiceerde in 2022 een verslag van hun onderzoek naar het gebruik van geavanceerde technologie in het justitiedomein.[6] Zij verwachtte voorafgaand aan het onderzoek dat er enig toezicht en democratische controle zou plaatsvinden op het gebruik van nieuwe technologieën in het justitiedomein in het algemeen en door de politie in het bijzonder. Uit hun onderzoek bleek echter het tegendeel.

---

1 Rosenthal 2007.

2 In dit hoofdstuk richt ik me op het technologiegebruik door de politie in algemene zin. Het evenwicht der machten in concrete casuïstiek – onder andere in het strafproces – is al aan de orde gekomen in hoofdstuk 27.

3 https://www.nrc.nl/nieuws/2018/01/11/de-besliscomputer-disciplineert-iedereen-ook-de-rechter (voor het laatst geraadpleegd op 10 augustus 2022).

4 AP 2023.

5 https://www.bitsoffreedom.nl/2021/07/31/goed-nieuws-politie-neemt-onze-wob-over-databank-voor-gezichtsherkenning-niet-in-behandeling/ (voor het laatst geraadpleegd op 11 augustus 2023).

6 De House of Lords is enigszins te vergelijken met de Eerste Kamer in Nederland. Het is ook een senaat, maar dan niet indirect gekozen zoals in Nederland. Het huis bestaat daardoor uit edelen, rechters en geestelijk leiders die meestal voor het leven zijn benoemd.

> *'Instead, we uncovered a landscape, a new Wild West, in which new technologies are developing at a pace that public awareness, government and legislation have not kept up with.'*[7]

Het gebrek aan politieke betrokkenheid en controle wordt niet alleen veroorzaakt doordat politici niet op de hoogte zijn van de ontwikkelingen die plaatsvinden, maar ook doordat de kennis waarover men beschikt ontoereikend is om de verantwoordelijke minister hier goed op te bevragen.[8] Dit leidt ertoe dat veel zaken voor kennisgeving worden aangenomen. Dit is – in meer algemene zin – ook zichtbaar in de behandeling van wetgeving. In 2013 ging wetgeving voor het Systeem Risico Indicatie (SyRI) in de fraudebestrijding geruisloos door de Tweede Kamer.[9] In 2020 werd het systeem – dankzij een rechtszaak van een groep bezorgde burgers en maatschappelijke organisaties – door de rechter verboden, omdat het in strijd is met het EVRM.[10] Een ander voorbeeld is de Wet gegevensverwerking door samenwerkingsverbanden (WGS) in het kader van de aanpak van ondermijnende criminaliteit.[11] Het wetsvoorstel werd eind 2020 'haast schouderophalend' door de Tweede Kamer aangenomen, terwijl zowel de Raad van State als de AP stevige kritiek op het wetsvoorstel heeft geuit.[12] Volgens de AP gaat de WGS met betrekking tot het delen van persoonsgegevens nog verder dan het inmiddels beëindigde SyRI.[13] Het risico van massasurveillance ligt op de loer.[14]

Bij voorgaand patroon moet worden opgemerkt dat het langzamerhand aan het veranderen is. In de afgelopen jaren hebben de Kamercommissies van zowel Justitie en Veiligheid als Digitale Zaken de minister van Justitie en Veiligheid af en toe (vrij gedetailleerd) bevraagd op het technologiegebruik door de politie. Daarnaast worden ontwikkelingen actiever met de Tweede Kamer gedeeld, zoals het inzetkader voor gezichtsherkenningstechnologie politie (zie ook hoofdstuk 14). Deze positieve verandering neemt echter niet weg dat de technologische revolutie nog steeds betrekkelijk 'stil' is en de politiek vooralsnog niet of nauwelijks invulling geeft aan haar controlerende rol waar het gaat om het gebruik van digitale technologie door de overheid in het algemeen en de politie in het bijzonder. Men wordt in de regel pas goed wakker nadat er

7 House of Lords 2021.
8 Zie Passchier 2021; Verhoeven 2023.
9 Buitenweg 2021; Verhoeven 2023.
10 https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:865 (voor het laatst geraadpleegd op 10 augustus 2022).
11 Deze wet is bedoeld om de aanpak van ondermijnende criminaliteit te versterken door middel van ruimere mogelijkheden voor het delen van informatie binnen samenwerkingsverbanden, waaronder zorg- en veiligheidshuizen, regionale informatie- en expertisecentra, de infobox crimineel en onverklaarbaar vermogen en het financieel expertisecentrum. Het wetsvoorstel is op dit moment aanhangig in de Eerste Kamer.
12 Verhoeven 2023.
13 De minister van Justitie en Veiligheid heeft – naar aanleiding van de kritiek – een algemene maatregel van bestuur (AMvB) opgesteld ter aanvulling op het wetvoorstel. Deze AMvB moet voorzien in heldere grondslagen en stevige waarborgen voor gegevensuitwisseling door samenwerkingsverbanden. De AMvB is in februari 2023 in (internet)consultatie gegaan.
14 https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-adviseert-eerste-kamer-neem-wgs-niet-aan (voor het laatst geraadpleegd op 22 januari 2023).

negatieve berichtgeving over een vorm van algoritmische besluitvorming naar buiten is gekomen.[15] Met betrekking tot de politie is de al vaker aangehaalde sensing proeftuin in Roermond illustratief: het kritische rapport van Amnesty International en de mediaberichtgeving hierover waren aanleiding voor een bespreking in de Tweede Kamer.[16] Tijdens deze bespreking deed zich een situatie voor die onderdeel is van een ander patroon dat behandeling verdient: het overheidsbestuur schuift diens verantwoordelijkheid voor het beschermen van mensenrechten bij het gebruik van digitale technologie door naar de rechter.

> **'Het is aan de rechter om hier een oordeel over te vellen'**
> Tijdens de bespreking van de sensing proeftuin in de Tweede Kamer kreeg de toenmalige minister van Justitie en Veiligheid een vraag over de rechtmatigheid van het gebruik van het land van herkomst van het voertuig in het algoritme. De minister ontweek het geven van een inhoudelijk antwoord op deze vraag door te stellen dat het aan de rechter is om hier een oordeel over te vellen indien een betrokken burger dit wil aanvechten.[17] De vraag is echter: wie vecht dit aan? Zeker voor kwetsbare burgers geldt dat zij in de regel niet zomaar de positie en middelen hebben om dit te doen.[18] 'The people most at risk of harm from big data systems are often those least able to contest the outcomes', aldus Sarah Brayne.[19] Kathalijne Buitenweg belicht de andere kant van deze medaille: 'Voorspellende algoritmen blijken in de praktijk vooral gunstig uit te pakken voor mensen die het toch al getroffen hebben in het leven.'[20] Anders gezegd: degenen die het best in staat zijn om het gebruik van een algoritme aan te vechten, hebben hier de minste noodzaak toe.

Het voorgaande leidt tot de vraag wie eigenlijk nog meekijkt met de uitvoerende macht. Het gewenste evenwicht der machten binnen de *trias politica* komt in het tijdperk van AI onder druk te staan.[21] Dit doet zich ook voor bij datagedreven politiewerk. De uitvoerende macht – in dit geval de politie – is dominant; daar ligt de macht. Die heeft de data, de infrastructuur, de expertise et cetera (zie hoofdstuk 23).[22] Politici en magistraten hebben steeds minder grip op de technologische ontwikkelingen binnen de

15 Zie ook Verhoeven 2023.
16 Amnesty International 2020.
17 Zie https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2020D51906&did=2020D51906 (voor het laatst geraadpleegd op 10 augustus 2022).
18 Het voorbeeld van Khalid uit het vorige hoofdstuk – het gaat dan om de inzet van een advocaat om van de Top600 lijst af te komen – is vermoedelijk eerder de uitzondering dan de regel.
19 Brayne 2021:144. Zie ook: Van der Knaap 2022.
20 Buitenweg 2021: 220.
21 Februari 2023; Passchier 2021.
22 Hierbij moet worden opgemerkt dat de politie in toenemende mate verweven raakt met de private sector die haar voorziet van onder andere expertise en systemen. Dit is niet nieuw, maar omdat bedrijven de algoritmen ontwerpen die de politie gebruikt voor onder andere socialemediamonitoring is er sprake van een andere – meer vergaande – invloed dan bij de software van voorheen (zie ook Februari 2023).

politie.[23] Zij zijn onvoldoende in staat om hun controlerende rol te vervullen. Het evenwicht der machten raakt hierdoor verstoord. Dit doet afbreuk aan de legitimiteit van datagedreven politiewerk, want degenen die sturen met data moeten (democratisch) worden gecontroleerd.[24] Het gebrek aan (democratische) controle heeft niet alleen te maken hebben met het gebrek aan kennis en interesse bij volksvertegenwoordigers en het gegeven dat de rechterlijke macht niet of te laat in beeld komt, maar ook met een gebrek aan transparantie dat bij het gebruik van AI en algoritmische besluitvorming op de loer ligt.

Gebrekkige transparantie rondom politieel technologiegebruik
Het gebruik van opkomende technologieën door de politie gaat gepaard met gebrekkige transparantie. Dit bemoeilijkt de verantwoording over politieoptreden, want transparantie is een randvoorwaarde voor deze verantwoording.[25] Verantwoording over politieoptreden is echter essentieel voor democratisch politiewerk.[26] De politie moet kunnen uitleggen hoe beslissingen tot stand komen. Dit is een beginsel van behoorlijk bestuur (motiveringsbeginsel).[27] Het is daarom van belang om nader in te gaan op het gebrek aan transparantie. Ik behandel twee redenen die hieraan ten grondslag liggen.[28]

De eerste en voornaamste reden is geheimhouding. Dit wil zeggen dat er aan politiek en samenleving geen inzicht wordt gegeven in de technologie die de politie gebruikt en/of in de wijze waarop deze technologie werkt.[29] Deze geheimhouding heeft twee redenen. De eerste reden heeft te maken met het doel waarvoor de politie technologie (ook) gebruikt, namelijk: handhaven en opsporen. Openheid met betrekking tot de gebruikte technologie kan op gespannen voet staan met het opsporings- en handhavingsbelang.[30] Dit argument is in de afgelopen jaren diverse keren door ministers gebruikt om in de Tweede Kamer geen openheid van zaken te geven over het technologiegebruik door de politie.[31] In november 2022 zijn er door de vaste Kamercommissie Digitale Zaken veel vragen aan de minister van Binnenlandse Zaken en Koninkrijksrelaties gesteld over onder andere het technologiegebruik door de politie. Toen werd gevraagd naar een overzicht van de software die door de politie wordt gebruikt voor proactief politiewerk gaf de minister aan dat – omwille van de handhavings- en opspo-

23 https://www.groene.nl/artikel/op-de-vlucht-voor-de-vrijheid (voor het laatst geraadpleegd op 10 augustus 2022).
24 ROB 2021.
25 Brayne 2021.
26 Egbert & Leese 2021.
27 WRR 2016.
28 Daarmee is deze paragraaf niet volledig. Zie voor een meer volledige uitwerking: Wessels 2023.
29 Zie ook Brayne 2021.
30 Zie ook Osinga et al. 2022.
31 In de fraudebestrijding in de sociale zekerheid is hier ook sprake van. Toen burgerrechten organisaties op basis van de Wet openbaarheid van bestuur (Wob) inzage vroegen in het algoritme van SyRI, kregen zij ook een afwijzing met verwijzing naar het belang van opsporing en vervolging. Zie ook het Wob-verzoek Systeem Risico Indicatie, 12 december 2016.

ringstaken – terughoudend moet worden omgegaan met precieze informatie over het technologiegebruik door de politie.[32] Twee jaar eerder werd er – naar aanleiding van het rapport van Amnesty International – in de Tweede Kamer gesproken over de sensing proeftuin in Roermond. Door Tweede Kamerleden werd gevraagd om een lijst van factoren die de risicoscore van een auto en inzittenden bepalen. De minister van Justitie & Veiligheid gaf aan deze lijst niet openbaar te kunnen maken, want dit zou het opsporings- en handhavingsbelang doorkruisen.[33] Een ander voorbeeld betreft de software die wordt gebruikt voor de hackbevoegdheid van de politie, die wordt uitgeoefend door het DIGIT van de landelijke eenheid.[34] In de Tweede Kamer werd gevraagd naar welke software de politie gebruikt.[35] De ministers van Binnenlandse Zaken & Koninkrijksrelaties en Justitie & Veiligheid gaven aan hier geen informatie over te kunnen geven vanwege onaanvaardbare risico's voor de betreffende bevoegdheid en het opsporingsbelang.[36] Hoewel dit ten aanzien van dergelijke software te begrijpen is, leert de ervaring (dus) dat deze manier van redeneren ten behoeve van geheimhouding veel breder wordt toegepast. Niet alleen door de ministers, maar ook door de politie zelf. Toen er aan de politie vragen werden gesteld over het gebruik van software van het Amerikaanse bedrijf Palantir, was men bijvoorbeeld niet erg genegen om openheid van zaken te geven.[37]

De tweede reden voor geheimhouding heeft te maken met bedrijfsgeheim. In hoofdstuk 24 is aangegeven dat de discretionaire macht voor een deel verschuift van de uitvoerende professionals naar de bedrijven die systemen en algoritmen ontwerpen. In Nederland is hier beperkt sprake van, omdat software in behoorlijke mate in eigen beheer wordt ontwikkeld, maar dit neemt niet weg dat het zich wel voordoet. De ervaringen in de VS wijzen uit dat het vrijwel onmogelijk is om inzicht te krijgen in de algoritmen die in software van bedrijven worden gebruikt, omdat zij zich beroepen op het bedrijfsgeheim.[38] Een algoritme wordt dan gedefinieerd als intellectueel eigendom en via die weg afgeschermd. Dit past in principe niet bij de publieke sector.

32 Zie hiervoor het verslag van de bijeenkomst van de vaste Kamercommissie Digitale Zaken die heeft plaatsgevonden op 14 november 2022: https://www.tweedekamer.nl/kamerstukken/commissieverslagen/detail?id=-2022Z21400&did=2022D50031 (voor het laatst geraadpleegd op 3 januari 2023). De vraag naar een overzicht van software/tools is overigens in relatie tot verschillende doeleinden (breder dan proactief politiewerk) gesteld.

33 Zie https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2020D51906&did=2020D51906 (voor het laatst geraadpleegd op 10 augustus 2022).

34 Zie in het kader van het gebruik van hacksoftware door overheden ook de berichtgeving over het gebruik van Pegasus software van het Israëlische bedrijf NSO Group. Zie Sartor & Loreggia (2022) over de (negatieve) gevolgen van het gebruik van deze software voor mensenrechten en democratie.

35 Het betreft in ieder geval geheime commerciële software waarbij de leverancier toegang kan krijgen tot de (middels de hack) verkregen gegevens. Hier zijn door zowel de Inspectie Justitie en Veiligheid (2022) als de Hoge Raad (2022) kritische opmerkingen over gemaakt.

36 Zie de brief van 23 juni 2022 betreffende de beantwoording van vragen inzake het gebruik van hacksoftware, zoals Pegasus, in Nederland.

37 https://fd.nl/achtergrond/1359235/geen-belegger-weet-wat-databedrijf-palantir-eigenlijk-doet (voor het laatst geraadpleegd op 10 augustus 2022).

38 Ávila, Hannah-Moffat & Maurutto 2021; Brayne 2021; Egbert & Leese 2021; Ferguson 2017a.

> *'Modern governance should not be shrouded behind impenetrable computer code and redundancy. If a tool is procured by a public agency, it should require ongoing documentation and have clear data and records ownership practices.'*[39]

Voor de hacksoftware die de politie in Nederland gebruikt – of dit nu Pegasus is of andere software – geldt bijvoorbeeld dat onduidelijk is hoe de software precies werkt. Dit bemoeilijkt onder andere de taak van de Inspectie Justitie & Veiligheid die toezicht houdt op de uitoefening van de hackbevoegdheid door de politie.[40] Dit illustreert het verantwoordingsrisico.

De tweede oorzaak voor gebrekkige transparantie omtrent technologiegebruik heeft te maken met de complexiteit van technologie. Het gaat dan in het bijzonder om het gebruik van zelflerende algoritmen: de werking van een zelflerend algoritme onttrekt zich op den duur aan het zicht en vooral aan het vermogen van mensen.[41] Een zelflerend algoritme gaat, mede op basis van feedback uit de omgeving, in grote mate diens eigen weg en verschilt op het gebied van transparantie daarmee van een algoritme dat 'hard-coded' is geprogrammeerd (zie hoofdstuk 5).[42]

Het ondoorzichtige algoritme van het CAS

Uit empirisch onderzoek komt naar voren dat de intelligencemedewerkers die de uitkomsten van het CAS moesten vertalen naar een advies aan de basisteams de datawetenschappers geregeld vroegen om toelichting op de totstandkoming van de uitkomsten van het CAS.[43] De betrokken datawetenschappers gaven vervolgens aan dat de gebruikte technieken voor patroonherkenning te complex waren als gevolg waarvan het zelflerende algoritme ondoorzichtig was. Er kon wel inzicht worden gegeven in variabelen (predictoren), maar niet in de precieze totstandkoming van de uitkomsten. Dit voldeed niet aan de behoefte van de intelligencemedewerkers en die gaven het op een gegeven moment op.

Een zelflerend algoritme is – zeker met de ontwikkeling naar *explainable AI*[44] – nog wel te expliciteren, maar dit is nog iets anders dan begrijpen wat er plaatsvindt. Anders gezegd: je kunt wel onder de motorkap kijken, maar de vraag is of je snapt wat je ziet.

39 Brayne 2021: 146
40 Inspectie Justitie & Veiligheid 2022.
41 Zie ook Hordijk & Lindsen 2023.
42 Hierbij doen zich verschillen voor tussen typen algoritmen (zie hoofdstuk 5). Vooral diepe, neurale netwerken zijn (vanwege hun complexiteit) ondoorzichtig. Het zijn grote modellen die vrijwel automatisch worden geconfigureerd. Zie verder: Maggiori 2023; Mannes 2020.
43 Zie Waardenburg 2021; zie ook de Algemene Rekenkamer 2022 over de transparantie van het CAS.
44 Zie Testerink, Nieuwenhuizen & Bex (2023) voor de inspanningen die in het Nationaal Politielab AI worden verricht om te komen tot uitlegbare AI, zodat de datawetenschapper of eindgebruiker meer inzicht krijgt in het keuzeproces van een AI-toepassing. Men maakt onder andere gebruik van een tool – Explabox – waarmee machine learning modules kunnen worden geanalyseerd. Op deze wijze kan in kaart worden gebracht door welke factoren de output van een machine learning algoritme wordt beïnvloed.

De kracht van een zelflerend algoritme is ook diens zwakte: doordat de cognitieve vermogens van mensen ruimschoots worden overtroffen, kunnen mensen niet of nauwelijks interpreteren op welke wijze een zelflerend algoritme tot uitkomsten is gekomen.[45] Transparantie vereist echter niet alleen het kunnen benaderen of expliciteren van een zelflerend algoritme, maar ook het begrijpen ervan.[46]

> *'How to make algorithms transparent however, is a multi-faced issue. Transparency is restricted by complexity — a random forest algorithm can be explained, but it may not be understood — on a practical level they can have hundreds of thousands of lines of code.'*[47]

Kortom: een zelflerend algoritme is *inherent ondoorzichtig*. Het is tot op zekere hoogte een black box: er gaat wat in en komt wat uit, maar wat daartussen nu precies gebeurt blijft onduidelijk.[48] Een politieorganisatie die steeds meer gebruikmaakt van AI-systemen loopt het risico dat zij na verloop van tijd niet meer kan uitleggen hoe bepaalde uitkomsten zijn gegenereerd. Als er op basis van deze uitkomsten wordt opgetreden, ontstaat *black box policing*.[49]
Tegen het gebrek aan transparantie van zelflerende algoritmen – als gevolg van bovengenoemde redenen – is ook het een en ander in te brengen. Zo wordt door sommigen gesteld dat het menselijk brein ook een black box is:[50] de redenen voor menselijke beslissingen zijn vaak niet zo expliciet, bijvoorbeeld als het gaat over proactieve controles door politiemensen. Deze invalshoek hebben we eerder gezien (zie hoofdstukken 26 en 28): worden algoritmen beoordeeld op basis van een ideaal van accuraatheid, objectiviteit en transparantie of op basis van de huidige praktijk van een 'onvolkomen' menselijk brein? Daarnaast wordt er geregeld op gewezen dat het gebrek aan transparantie wordt ondervangen door het gegeven dat niet het algoritme, maar de mens beslist. Dit bracht de minister van Justitie & Veiligheid ook naar voren in een brief aan de Tweede Kamer over het gebruik van AI bij de politie: de *human-in-the-loop* wordt gezien als een waarborg voor transparantie en kwaliteit.[51] Naar mijn mening overtuigen deze tegenargumenten niet. Het menselijk brein is weliswaar ook een black box, maar een politieagent is in de rechtszaal (wanneer nodig) te bevragen op bijvoorbeeld diens onderbouwing voor een redelijke verdenking, maar bij een algoritme is dit niet of in veel mindere mate het geval. De menselijke tussenkomst kan worden gezien als een

45 Hung & Yen 2021. Dit geldt in het bijzonder voor diepe, neurale netwerken: je kunt nog wel begrijpen wat de eerste laag doet, maar hoe dieper je komt, des te lastiger het wordt om de logica van de berekeningen te begrijpen (zie Maggiori, 2023).
46 Vestby & Vestby 2019.
47 Bland 2020: 150.
48 O'Neil 2016; Pasquale 2016.
49 Wilson 2018.
50 Berk 2021.
51 Brief 'Artificiële intelligentie bij de politie' van de minister van JenV aan de TK van 3 december 2019.

belangrijk gegeven,[52] maar dit neemt niet weg dat er alsnog sprake is van algoritmische besluitvorming (zie hoofdstuk 24): de uitvoer van een algoritme wordt meegenomen in een menselijk besluitvormingsproces en beïnvloedt dit besluitvormingsproces ook. Sterker nog, als gevolg van *automation bias* kan er bij mensen een neiging ontstaan om de besluiten of suggesties van een AI-systeem blindelings over te nemen.[53] Een AI-systeem neemt dan feitelijk zelf de beslissing.[54] Het is dus van belang dat uitgelegd kan worden hoe een algoritme tot de uitkomst is gekomen en hoe die uitkomst het optreden heeft beïnvloed.[55] Op dit moment is hier – voor wat betreft zelflerende algoritmen – veelal onvoldoende sprake van.[56]

Kortom: geheimhouding en complexiteit van technologie doen afbreuk aan de openheid die kan worden gegeven met betrekking tot technologiegebruik door de politie.[57] Dit is een risico voor het vertrouwen van burgers in het optreden van de politie. Onderzoek laat in algemene zin zien dat burgers algoritmische beslissystemen negatief beoordelen als niet kan worden uitgelegd hoe het systeem tot diens uitkomsten komt.[58] De gebrekkige transparantie ondermijnt daarnaast het evenwicht der machten in onze democratische rechtsstaat, omdat controle wordt bemoeilijkt.[59]

Waarborgen voor het evenwicht der machten

De conclusie van de twee voorgaande paragrafen is dat we vooralsnog niet gerust kunnen zijn op de aanwezigheid van voldoende waarborgen voor verantwoord gebruik van opkomende technologieën door de politie. De wetgevende en controlerende macht pakt het nog onvoldoende op, het bestuur verschuilt zich te veel achter de rechtspraak en de rechtspraak komt alleen in positie als burgers iets aanvechten, wat vrijwel niet het geval is. Dit roept de vraag op wat er door wie wordt gedaan om waarborgen voor verantwoord technologiegebruik en evenwicht der machten te realiseren.

52 Zie voor een ander perspectief op de human-in-the-loop het artikel van Testerink, Nieuwenhuizen & Bex (2023) die aangeven dat vaak onduidelijk is *waarom* deze human-in-the-loop wenselijk is. Er is volgens hen sprake van ongemak over autonomie van (AI) systemen, terwijl maar zelden concrete problemen van autonome AI-systemen worden benoemd die specifiek worden veroorzaakt door autonomie en niet door bijvoorbeeld een bias, onnauwkeurigheid of programmeerfout. Zij stellen ook de vraag waarom de autonomie van een politiehond blijkbaar minder problematisch is dan de autonomie van een robothond. Anders gezegd: waarom wantrouwen we een systeem meer dan een dier of mens?

53 Buitenweg 2021; McDaniel & Pease 2021b. Hierbij moet als nuancerende opmerking worden gemaakt dat de mate waarin uitkomsten van algoritmen worden overgenomen door uitvoerende professionals kan verschillen. Automation bias is zeker geen gegeven. Zie bijvoorbeeld Meijer, Lorenz & Wessels (2021) over de verschillen tussen Amsterdam en Berlijn voor wat betreft het gebruik en de invloed van predictive mapping.

54 Zie ook Testerink, Nieuwenhuizen & Bex 2023.

55 Zie ook Rathenau Instituut 2023.

56 Hierbij moet voor de volledigheid wel worden opgemerkt dat de politie in Nederland op dit moment op kleine schaal gebruikmaakt van zelflerende algoritmen (zie ook Schuilenburg & Soudijn, 2021).

57 Zie ook Shapiro 2017.

58 Schiff, Schiff & Pierson 2021; zie ook Grimmelikhuijsen 2022.

59 Zie Passchier 2021 voor een brede beschouwing (breder dan de politie).

Bij het beantwoorden van deze vraag begin ik in Europa. Door de Europese Commissie is een verordening opgesteld voor het reguleren van het gebruik van AI: de *AI Act*. De AI Act is wereldwijd de eerste poging om te komen integrale wetgeving die voor alle sectoren geldt met expliciete verantwoordelijkheden voor zowel ontwikkelaars als gebruikers van AI-systemen. In de AI Act is een risicogerichte indeling gemaakt in verschillende typen AI-systemen. Systemen met een hoog risico zijn voor de politie het meest relevant.[60] Als gevolg van de AI Act krijgen politiekorpsen in Europa – naar verwachting vanaf 2024 – te maken met meer regulering van en toezicht op de AI-systemen die zij gebruiken.[61] Het gaat dan vooral om de hoogrisicosystemen die zij gebruiken voor 1) het voorspellen van criminaliteit, 2) profileren van personen tijdens opsporing van strafbare feiten, en 3) misdaadanalyses waarmee grote hoeveelheden data worden geanalyseerd.[62] De AI Act gaat uit van een nationale toezichthoudende autoriteit die in samenwerking met andere autoriteiten toeziet op naleving van de AI Act. Dit is in ons land de AP.[63]

De AP brengt ons op de situatie op nationaal niveau. Vanaf 2023 functioneert de AP als de Nederlandse 'algoritmewaakhond' waarbij de focus ligt op transparantie, discriminatie en willekeur.[64] De AP gaat zich vooral richten op risico's die sectoren en domeinen overstijgen. In de beginperiode ligt de nadruk op het signaleren van risicovolle algoritmen, het bundelen van kennis en het verder vormgeven van samenwerking. De AP werkt domeinoverstijgend. In het politiedomein is er een 'eigen' toezichthouder: de eerdergenoemde Inspectie Justitie & Veiligheid. De inspectie houdt toezicht op de taakuitvoering door de politie. Door de minister van Justitie & Veiligheid is in 2019 aangegeven dat het toezicht op onder andere AI-toepassingen – ten behoeve van de taakuitvoering – hier onderdeel van is.[65] Het is echter onduidelijk in welke mate de inspectie hierop gericht en hiervoor toegerust is. Er zijn vooralsnog geen voorbeelden waarin de inspectie het toezicht op technologiegebruik door de politie heeft ingevuld, behalve het eerdergenoemde toezicht op de hackbevoegdheid van de politie.

60 Zie ook Schuilenburg & Wessels 2022.

61 De Europese Raad heeft eind 2021 ingestemd met het algemene standpunt van de lidstaten. Het Europees Parlement stemde in juni 2023 – via geconsolideerde amendementen – over zijn standpunt. Op basis hiervan zijn de onderhandelingen gestart om de wetgeving af te ronden. Dit zal vermoedelijk nog leiden tot substantiële wijzigingen, waaronder een mogelijke uitbreiding van de lijst met verboden AI-systemen en het toevoegen van verplichtingen voor algemene AI-modellen, zoals ChatGPT. Zie hiervoor: Madiega 2023.

62 De AI Act neemt de risico's van AI – meer dan diens mogelijkheden – als vertrekpunt. Dit kan – mede vanwege de strenge eisen (zie Hordijk & Lindsen 2023) – innovatie in het domein van onder andere de handhaving beperken. Het VK lijkt in zijn regulering bijvoorbeeld te kiezen voor minder strakke regulering van AI en biedt daarmee meer ruimte voor het benutten van de mogelijkheden. Dit roept tegelijkertijd de vraag op of de risico's van AI voldoende kunnen worden beheerst (deze beheersing is overigens met de AI Act zeker geen gegeven). Zie verder: https://policinginsight.com/features/opinion/how-the-uk-is-getting-ai-regulation-right/ (voor het laatst geraadpleegd op 11 augustus 2023).

63 Er is daarnaast een Samenwerkingsplatform Digitale Toezichthouders (SDT) waarin de AP participeert.

64 Zie de brief van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties aan de Tweede Kamer over de inrichting van de algoritmetoezichthouder van 22 december 2022.

65 Brief 'Artificiële Intelligentie bij de politie' van de minister van JenV aan de TK van 3 december 2019.

Van het nationale niveau gaan we naar de politieorganisatie. Te midden van de vooralsnog gebrekkige (democratische) controle op technologiegebruik door de politie is het vooral aan de politie zelf om ervoor te zorgen dat datagedreven politiewerk voldoet aan de waarden en normen van de democratische rechtsstaat. De minister van Justitie & Veiligheid gaf in 2019 nog expliciet aan dat de politie in het kader van het gebruik van AI haar eigen 'strengste criticaster' is.[66] Het moge duidelijk zijn dit uitgangspunt zich moeizaam verhoudt tot het belang van het evenwicht der machten in een democratische rechtsstaat. Het roept tegelijkertijd de vraag op hoe de politie invulling geeft aan het interne toezicht. In dit kader moet erop worden gewezen dat er binnen de politie uiteenlopende organisatieonderdelen en functionarissen zijn die zich bezighouden met toezicht op onder andere de gegevensverwerking, zoals de Gegevensautoriteit bij de staf van de korpsleiding en privacyfunctionarissen in de eenheden. Daarnaast zijn er in de afgelopen jaren diverse initiatieven ontwikkeld die ervoor moeten zorgen dat het technologiegebruik door de politie voldoet aan de waarden en normen van de democratische rechtsstaat. Er zijn nieuwe functies ingericht ten behoeve van de juridische en ethische aspecten van AI.[67] Het betreft daarnaast diverse beleidsinitiatieven en nieuwe gremia, zoals het uitvoeringskader privacy en security by design,[68] het kwaliteitskader big data,[69] ethiektafels,[70] een ethische commissie[71] en de inrichting van een 'portefeuille' ethiek & privacy.[72] Ook kan worden gedacht aan het ontwikkelen en gebruiken van instrumenten, zoals een data protection impact assessment (DPIA),[73] de opzet van een algoritmeregister[74] en het toetsen van de kwaliteit van algoritmen.[75] Deze ontwikkelingen bevinden zich in diverse stadia: het kwaliteitskader wordt bijvoorbeeld al enkele jaren gebruikt, terwijl het algoritmeregister op dit moment in ontwikkeling is.[76]

66 Idem.
67 Dit baseer ik op vacatures die zijn gepubliceerd.
68 Politie 2018.
69 OM en Politie 2020.
70 Politie 2019.
71 Dit initiatief is genoemd in het deelrapport over de politie in het kader van het parlementaire onderzoek naar mogelijkheden van de wetgever om discriminatie tegen te gaan (Eerste Kamer, 2022).
72 Zie hiervoor *Begroting en beheerplan 2021-2025* van de politie, pagina 16.
73 Dit wordt binnen de politie een gegevensbeschermingseffectbeoordeling (GEB) genoemd. Het uitvoeren van een GEB komt bij nieuwe toepassingen c.q. systemen naar mijn indruk steeds vaker voor, maar was zeker in het verleden geen (uitgevoerde) standaardprocedure. Uit het onderzoek van Prins (2020) komt bijvoorbeeld naar voren dat de politie – naar eigen zeggen – bij vele technologieprojecten geen GEB heeft uitgevoerd. Dit geldt onder andere voor de bekritiseerde sensing proeftuin in Roermond.
74 Testerink, Nieuwenhuizen & Bex 2023.
75 Zie www.ftm/artikelen/politie-stopt-met-voorspellend-algoritme-geweld (voor het laatst geraadpleegd op 29 augustus 2023).
76 In dit register wordt onder andere opgenomen binnen welke risicoclassificatie een algoritme valt (in lijn met de AI Act), wie er betrokken zijn bij de ontwikkeling van een algoritme en hoe een algoritme wordt gemonitord en/of wordt geëvalueerd. Een dergelijk register geeft burgers en maatschappelijke organisaties inzicht in de algoritmen die de politie gebruikt, al zal het opnieuw de vraag zijn welke mate van openheid de politie door middel van dit algoritmeregister gaat geven.

Op basis van het voorgaande kan in algemene zin worden geconcludeerd dat er een ontwikkeling gaande is naar meer evenwicht tussen de machten en naar meer waarborgen binnen de politie. Dit is een positieve ontwikkeling, maar het is de vraag of het genoeg is. Dit heeft in de eerste plaats een fundamentele reden die een veel bredere strekking heeft dan het politiedomein. Ik citeer Maxim Februari in een essay over 'menselijk recht in tijden van datasturing':

> *'Het zijn nuttige stappen… Heel nuttig. Alleen houden deze stappen nog geen rekening met de verschuivingen in het constitutionele bestel zelf en de noodzaak om dat bestel opnieuw uit te vinden.'*[77]

De AI Act, algoritmetoezicht, algoritmeregisters, beleidskaders en dergelijke maatregelen zijn onderdeel van wat Februari *constitutionaliseren* noemt. Een nieuwe werkelijkheid wordt met oude methoden benaderd. Er wordt getracht aan de structuren van de democratische rechtsstaat te sleutelen in een situatie die niet vanuit die structureren is ontstaan. Anders gezegd: constitutionaliseren gaat '… eraan voorbij dat de overheid niet langer hiërarchisch is, dat ze in deze nieuwe eeuw bestaat uit netwerken en informatiestromen – en dat niemand, geen enkele instantie, die informatiestromen nog overziet. Je kunt het toezicht op de digitalisering wel willen overlaten aan de structuren van de oude overheid, maar die overheid is er in feite niet meer, die is vervangen.'[78] Februari roept de politieke gemeenschap, de rechtsgemeenschap, op om digitaal wakker te worden en te verkennen hoe de rechtsstaat zich in de nieuwe wereld moet ontwikkelen. Zijn essay maakt tegelijkertijd duidelijk dat antwoorden op deze vraag nog niet voorhanden zijn.

De tweede reden voor twijfel doet zich binnen het proces van constitutionaliseren voor. Dit proces vat ik hierbij breed op, wat impliceert dat ook de waarborgen binnen de politie hieronder vallen. De politie in Nederland investeert in allerlei waarborgen voor verantwoord gebruik van digitale technologie in het algemeen en AI in het bijzonder. Dit is een noodzakelijke ontwikkeling die waardering verdient. Deze waarborgen zijn in de regel echter (nog) te vrijblijvend en vooral te reactief.[79] Zo is een kwaliteitskader big data ongetwijfeld een nuttig instrument, maar het is – volgens het OM en de politie – geen voorschrijvend instrument, maar meer een hulpmiddel dat kan worden gebruikt bij het opzetten van concrete projecten waarin big data dan wel AI wordt toegepast.[80] Het zijn maatregelen die in taal de indruk van stevigheid geven ('kader'),

77 Februari 2023: 115.

78 Idem: 102.

79 Hierbij moet worden opgemerkt dat dit een algemene constatering is ('in de regel'), die geen recht doet aan alle technologische toepassingen die de politie gebruikt. Zo is het Inzetkader Gezichtsherkenningstechnologie Politie een stevig (doordacht) kader met een verplichtend karakter dat – naar mijn indruk – voorziet in de nodige waarborgen (zie Politie, 2023; hoofdstuk 14). Deze waarborgen vloeien onder andere voort uit de procedure die bij iedere nieuwe inzet moet worden gevolgd om de inzet te toetsen en tot besluitvorming over de inzet te komen.

80 OM en Politie 2020. Zie voor het vrijblijvende karakter ook: Schermer & Galič 2023.

maar in de praktijk weinig garanties bieden ('hulpmiddel').[81] Reactief wil zeggen dat veranderingen in het gebruik van data en/of algoritmen geregeld worden geïnitieerd nadat er in media is bericht over de gebreken ervan.[82] Kortom: de waarborgen om te voldoen aan de waarden en normen van de democratische rechtsstaat zijn vooralsnog te kwetsbaar. Dit kan een politie in een democratische rechtsstaat zich niet veroorloven. De politie moet daarom zelf (nog) steviger opstaan voor de waarden van de rechtsstaat en bescherming van de samenleving.

81 Het kwaliteitskader bestaat uit een groot aantal checkvragen die de betrokkenen bij projecten dienen te beantwoorden. Zo ontstaat een risico-inschatting op basis waarvan maatregelen kunnen worden genomen. Hierbij wordt aangegeven dat er geen goede of foute antwoorden zijn. Tevens wordt benadrukt dat het kwaliteitskader geen methode is om specifiek en expliciet inzicht te krijgen in de integriteit, uitlegbaarheid en redelijkheid van de algoritmen zelf. Zie OM en Politie (2020).

82 Een voorbeeld is het uit gebruik nemen van het RTI-Geweld na een kritische publicatie van *Follow the Money* (zie hoofdstuk 19).

30 Politiewerk aan de horizon

De aanleiding voor dit boek was mijn vermoeden dat opkomende technologieën het politiewerk wezenlijk (gaan) veranderen. In dit boek heb ik dit vermoeden verkend. Er zijn verschillende onderwerpen de revue gepasseerd, die allemaal te maken hebben met technologische ontwikkelingen en hun invloed op de politie. In dit laatste hoofdstuk formuleer ik de belangrijkste bevindingen die voortvloeien uit deze verkenning.[1] Op basis hiervan keer ik terug naar de vraag waarmee dit boek begonnen is: hoe wezenlijk of fundamenteel zijn de veranderingen? Vervolgens reflecteer ik op de totstandkoming van dit boek.

De bevindingen in vijftien punten

1. Onze samenleving is in vergaande mate gedigitaliseerd. Digitalisering is een uitvloeisel van de derde industriële revolutie die wordt gekenmerkt door de opkomst van informatie- en communicatietechnologie. De personal computer kwam eerst ons leven binnen en daarna werd deze computer verbonden met een wereldwijd netwerk van computers, genaamd het internet. Na de eeuwwisseling kwamen socialenetwerksites op en werd de smartphone geïntroduceerd. Sinds die tijd is een groot deel van de samenleving een aanzienlijk deel van diens tijd online gaan doorbrengen: onze ogen zijn steeds meer op schermen gericht. Doordat de objecten van de digitale revolutie massaal zijn geadopteerd door burgers is er in de afgelopen vijftien jaar een volledig andere economische en (sociale) mediawerkelijkheid ontstaan, met nieuwe conventies en daarmee gepaard gaande menselijke gedragingen. Deze ontwikkeling schrijdt voort: er zijn steeds meer apparaten met het internet verbonden (Internet of Things). Daarnaast investeren de grote technologiebedrijven in een nieuwe, driedimensionale variant van het internet – de metaverse – waarbij gebruik wordt gemaakt van immersieve technologieën (zoals virtual reality). De voortschrijdende digitalisering heeft onder andere als gevolg dat steeds meer menselijke handelingen worden omgezet in data en deze data vervolgens worden gebruikt in andere processen en toepassingen. Dit wordt *dataficatie* genoemd. In het gebruik van data spelen algoritmen een cruciale rol. Een algoritme is een set van instructies die in computertaal (code) is vastgelegd, zodat een computer de instructies kan opvolgen. Inputdata worden op deze wijze – via een geautomatiseerde reeks van stappen – omgezet in outputdata. De instructies kunnen

1 Ik laat hierbij verwijzingen achterwege. Zie hiervoor de hoofdstukken waarin de betreffende inhoud is behandeld.

door mensen worden opgesteld. Dan is er sprake van een modelgedreven algoritme, ook wel expertsysteem genoemd. Dit was de eerste variant van *artificiële intelligentie* (AI) die in de praktijk is gebracht. Het is sinds ongeveer tien jaar echter ook mogelijk om de computer te laten leren van data, zodat deze het algoritme min of meer zelfstandig kan ontwikkelen. Dan is er sprake van een datagedreven algoritme, ook wel *machine learning* genoemd. De nieuwe methodologie van machine learning, de explosieve groei van de beschikbare data (dataficatie) en de (sterk) toegenomen rekenkracht hebben geleid tot de huidige doorbraak van AI. AI kan steeds meer taken verrichten die intelligentie zouden vereisen als mensen ze zouden uitvoeren. AI is uitgegroeid tot een van de grootste technologische innovaties die de wereld aan het veranderen. Het is een systeemtechnologie die qua ontwikkeling nog in de kinderschoenen staat: we zijn de mogelijkheden van AI nog maar net aan het ontdekken. In de verdere ontwikkeling van AI zullen mens en machine – onder andere in de uitvoering van werk in organisaties – steeds meer met elkaar verweven raken.

2. Het veiligheidsvraagstuk is in de afgelopen tien jaar door digitalisering wezenlijk veranderd. Er heeft een *crime change* plaatsgevonden: bestaande delicten hebben vrijwel allemaal een digitale component gekregen en er is een nieuwe categorie delicten bijgekomen. De digitale criminaliteit – bestaande uit gedigitaliseerde criminaliteit en cybercriminaliteit – vormt een steeds groter deel van de gehele criminaliteit. Het internet heeft zich niet alleen ontwikkeld tot een nieuwe gelegenheidsstructuur voor en hulpmiddel bij het plegen van criminaliteit, maar is tevens een ruimte geworden waarin allerlei andere immorele gedragingen van burgers plaatsvinden en worden versterkt. Deze *evil online* bestaat uit uiteenlopende gedragingen die in toenemende mate ook strafbaar worden gesteld (bijvoorbeeld *doxing*). Sociale media spelen daarnaast een rol in het toenemende maatschappelijke ongenoegen waar in Nederland sprake van lijkt te zijn. Dit ongenoegen kan zich – via onder andere toenemende spanningen tussen bevolkingsgroepen en anti-overheidsextremisme – manifesteren als een veiligheidsvraagstuk. Het gedigitaliseerde veiligheidsvraagstuk – waarmee ik verwijs naar zowel digitale criminaliteit als andere vormen van digitale onveiligheid – is voor de politie *geen* 'oude wijn in nieuwe zakken'. Dit wil zeggen dat de (relatief) nieuwe fenomenen waarmee de politie te maken heeft op onderdelen *andere kenmerken* hebben dan de fenomenen die de politie gewend is om aan te pakken. De nieuwe fenomenen hebben (tot op zekere hoogte) een de-territoriaal karakter. Zo liggen de locaties van dader(s) en slachtoffer(s) van digitale criminaliteit veelal niet in elkaars nabijheid. Een tweede kenmerk is anonimiteit: het internet stelt mensen in staat om in behoorlijke mate anoniem te blijven bij het uitvoeren van handelingen. Ook het schaalniveau is anders: digitale criminaliteit is veel meer schaalbaar dan traditionele criminaliteit. Een vierde en (voor hier) laatste kenmerk is de private context waarin digitale onveiligheid wordt gecreëerd: het gedrag van een dader is niet of nauwelijks zichtbaar in het publieke domein en daders ondervinden in veel mindere mate 'real-life' consequenties van hun handelen. Een tweede betekenis van 'private context' heeft te ma-

ken met het private eigendom van de kabels, servers, verbindingen, platformen et cetera. Dit is een wezenlijk verschil met het 'publieke' karakter van (veel) traditionele criminaliteit en heeft onder andere als consequentie dat er andere partners in beeld komen voor de aanpak van digitale criminaliteit.

3. In de komende jaren wordt de digitale onveiligheid vooral beïnvloed door AI. AI-systemen en 'Internet-of-Things'-apparaten zullen in toenemende mate doelwit worden van criminaliteit. Een meer zorgelijke ontwikkeling is echter het gebruik van AI bij het plegen van criminaliteit. Digitale criminaliteit wordt door het gebruik van AI *geraffineerder van aard en gemakkelijker te plegen*. De uitvoering van delicten zal in toenemende mate worden geautomatiseerd, wat impliceert dat de digitale technologie in toenemende mate een actor wordt in de uitvoering. Het gemak en de geraffineerdheid waarmee digitale criminaliteit kan worden gepleegd, zullen vermoedelijk leiden tot een verdere toename van digitale criminaliteit. AI zal ook op andere manieren de onveiligheid beïnvloeden. Een van de voornaamste vraagstukken die zich hierbij voordoet, is de opkomst van *deepfakes*. Deepfakes zullen niet alleen worden gebruikt voor het plegen van criminaliteit, maar ook een rol spelen in allerlei andere immorele online gedragingen. Met de opkomst van deepfakes gaat het verspreiden van desinformatie een nieuwe – meer zorgelijke – fase in. De betrouwbaarheid van informatie komt onder grote druk te staan. Dit maakt het moeilijker om in de samenleving consensus te bereiken over belangrijke kwesties en tast daarmee de democratische rechtsstaat aan.
4. De politiefunctie – de regulatieve functie in de samenleving, die is bedoeld om het gedrag van mensen in overeenstemming te houden of brengen met de normen en regels die binnen de samenleving gelden – bevindt zich in een *aanpassingsproces* om ook in de digitale ruimte (effectief) te kunnen functioneren. Dit is een stevig aanpassingsproces, omdat de traditionele, fysieke politiefunctie *zich niet zomaar laat 'omzetten'* naar een digitale variant. Het is – zoals eerder aangegeven – niet 'meer van hetzelfde'. In de digitale variant van de politiefunctie spelen diverse, deels nieuwe, partijen een rol. De politie is een van deze partijen. De rol van de politie in de aanpak van digitale criminaliteit heeft zich in de afgelopen jaren behoorlijk ontwikkeld, al moet het been nog verder worden bijgetrokken. In het (schemer)domein van allerlei andere immorele, online gedragingen is de politie vooralsnog meer handelingsverlegen dan in het domein van de digitale criminaliteit. In dit schemerdomein zal het aantal onwenselijke fenomenen echter eerder toe- dan afnemen. Generatieve AI – AI waarmee synthetische media worden geproduceerd – zal hierin een belangrijke rol spelen. De roep om meer online aanwezigheid en daadkracht van de politie zal toenemen. De (eventuele) komst van de metaverse zal deze roep verder versterken. De politie staat dus voor de opgave om haar positie in het digitale domein nader te bepalen en aan de gewenste positie invulling te geven.
5. De voortschrijdende digitalisering in de samenleving heeft niet alleen geleid tot een nieuw domein waarin de politiefunctie wordt uitgeoefend, maar leidt ook tot verandering in de wijze waarop de politiefunctie wordt uitgeoefend in zowel het fysieke als digitale domein. Digitalisering biedt nieuwe mogelijkheden in het kader

van de handhaving van de rechtsorde en het uitoefenen van sociale controle. Deze verkenning maakt duidelijk dat deze mogelijkheden door zowel de politie als anderen in toenemende mate worden benut. Dit leidt tot *technologisering van de politiefunctie*: het uitoefenen van (aspecten van) sociale controle door digitale technologie. Anders gezegd: digitale technologie wordt in toenemende mate een actor in het beïnvloeden van het gedrag van burgers teneinde dit gedrag in overeenstemming te brengen met de normen en regels die in de samenleving gelden. Dit is onder andere zichtbaar in de ontwikkeling naar 'slimme steden'. De technologisering van de politiefunctie is een fundamentele ontwikkeling die van invloed is op *hoe de rechtsstaat zich ontwikkelt* en dus alertheid vereist.

6. Binnen de technologisering van de politiefunctie vindt technologisering van het werk van de politie plaats. Deze verkenning laat ondubbelzinnig zien dat de politie in Nederland het gebruik van moderne, digitale technologieën in het politiewerk *heeft omarmd*. Er zijn en worden uiteenlopende toepassingen breed in de politieorganisatie geïmplementeerd. Er wordt daarnaast volop geëxperimenteerd met nieuwe toepassingen die mogelijk breed worden geïmplementeerd. Deze (algoritmische) toepassingen worden ingezet voor een breed pallet aan politietaken en voor uiteenlopende temporele oriëntaties: reconstrueren, real-time en voorspellen. De toepassingen maken vooralsnog in beperkte – maar groeiende – mate gebruik van 'moderne' AI.[2] De politie in Nederland investeert aanzienlijk in de randvoorwaarden die nodig zijn om gebruik te kunnen maken van opkomende, digitale technologieën in het algemeen en AI in het bijzonder. Het gaat dan onder andere om het aantrekken van de benodigde expertise en het realiseren van de technische infrastructuur. De politie in Nederland lijkt in internationaal verband een van de koplopers te zijn in deze ontwikkeling. Het is dan ook zeer aannemelijk dat het gebruik van AI door de politie in Nederland de komende jaren (aanzienlijk) toeneemt.
7. De technologisering van politiewerk verwijst naar de veranderende rol van technologie in de uitvoering van politiewerk. Digitale technologie heeft van oudsher een ondersteunende rol in de uitvoering van politiewerk, onder andere in de vorm van registratiesystemen. Onder invloed van het gebruik van opkomende, digitale technologieën – in het bijzonder AI – *is deze rol aan het veranderen* in een meer bepalende of vormende rol. Anders gezegd: van secundair naar (meer) primair. Van de randen van het politiewerk naar (ook) de kern. De veranderende rol van technologie in de uitvoering van politiewerk komt doordat technologie in toenemende mate *processen van betekenisgeving van politiemensen versterkt en deels ook overneemt*. Dit heeft gevolgen voor de vermogens die de politie inzet voor de uitvoering van politietaken. Het vermogen tot waarnemen (de ogen van de politie) en het vermogen tot informatie verwerken (het brein van de politie) worden door het gebruik

2 Met moderne AI wordt verwezen naar machine learning. Hierbij moet worden opgemerkt dat wat (niet) tot AI wordt gerekend vatbaar is voor discussie (zie ook De Kool, Vermeeren & Steijn, 2023). Hierbij moet worden beseft dat toepassingen kunnen bestaan uit onderdelen waarin gebruik wordt gemaakt van AI. Het is geen 'alles of niets'-kwestie.

van opkomende, digitale technologieën substantieel uitgebreid. Deze vermogens worden – tot op zekere hoogte – ontkoppeld van (het vermogen van) politiemensen. Dit is een fundamentele ontwikkeling: in het politiewerk aan de horizon ontstaan in toenemende mate betekenisgevers zonder hersenen en zonder lichaam.

8. De veranderende rol van data en technologie in het politiewerk heeft in zowel wetenschap als praktijk geleid tot gebruik van een nieuw (paraplu)begrip. In internationaal verband gaat het dan om *big data policing* of *data-driven policing*. In nationaal verband wordt de term *datagedreven politiewerk* (of variant hiervan) gebruikt. Deze terminologie doet vermoeden dat er sprake is van een nieuw politiemodel, vergelijkbaar met gebiedsgebonden politie of intelligencegestuurd politiewerk. Er is – naar mijn idee – in de (brede) politiepraktijk nog geen sprake van een nieuw politiemodel. Datagedreven politiewerk heeft wel de potentie om een nieuw politiemodel te worden. Dit politiemodel wordt gekenmerkt door 1) een breed in de politieoperatie ingebed proces van verzamelen, opslaan en analyseren van (digitale) data als basis voor en onderdeel van het optreden (dus niet alleen een sturingsmodel, ook een operationeel model) en 2) het gebruik van AI voor de sturing en uitvoering van het politiewerk in het algemeen en het proces van verzamelen, opslaan en analyseren van data in het bijzonder. De politie legt op dit moment een stevige basis voor datagedreven politiewerk, maar het zal – net als bij andere modellen van politiewerk – tijd kosten alvorens datagedreven werken in de breedte van het politiewerk is ingebed. De impact van technologie wordt op de korte termijn vaak overschat en op lange termijn juist onderschat. Ik denk dat dit ook geldt voor de invloed van AI op het politiewerk: de meest merkbare of zichtbare invloed van AI op het politiewerk ligt nog voor ons.
9. De sociaal-technologische politiepraktijken die in dit boek zijn behandeld, geven een eerste inkijk in de veranderingen die kenmerkend zijn voor *het politiewerk aan de horizon*. De dominantie van het werken op straat neemt af; het politiewerk aan de horizon heeft vaker het karakter van bureauwerk. De reactieve modus beweegt naar meer proactief optreden; in het politiewerk aan de horizon wordt vaker ingegrepen voordat het onheil is geschied. De lokale inbedding van het politiewerk verliest aan betekenis; in het politiewerk aan de horizon spelen de relaties tussen gebeurtenissen en de betrokken personen zich op grotere schaal af. De discretionaire ruimte in de uitvoering neemt af; in het politiewerk aan de horizon wordt een deel van de beslissingsruimte ingevuld door algoritmen en wordt informatiesturing dominanter. De politiemens krijgt een minder centrale rol in de uitvoering van politiewerk; in het politiewerk aan de horizon wordt technologie een actor.
10. In het politiewerk aan de horizon blijft politievakmanschap *cruciaal*. Politiemensen zullen meer gaan samenwerken met politiemachines. In die samenwerking ontstaat een vorm van hybride intelligentie. Politiewerk wordt dan uitgevoerd op een manier die geen van beide alleen kan realiseren. De samenwerking tussen politiemens en politiemachine impliceert dat het vakmanschap dat voor het politiewerk aan de horizon wordt gevraagd anders is dan het huidige vakmanschap. De politiemachine zal de politiemens niet vervangen, maar de politiemens die een politiemachine

gebruikt, vervangt wel degene *die dit niet doet*. Het gevraagde politievakmanschap omvat diverse aspecten. Het begint met een digitale mindset of oriëntatie: openstaan voor de mogelijkheden die opkomende technologieën jouw politiewerk bieden en bereid zijn om te investeren in de kennis om hierin 'bij te blijven'. Het gaat daarnaast om datageletterdheid, vaardigheid in softwaregebruik, analysevaardigheden, kennis van juridische aspecten van datagedreven politiewerk en de competentie om bij te dragen aan het ontwikkelen en functioneren van technologie in het algemeen en AI in het bijzonder.

11. De relevantie van datagedreven politiewerk voor de samenleving vloeit voort uit de belofte van effectiviteit. Op dit moment weten we niet of datagedreven politiewerk deze belofte waarmaakt of kan waarmaken. Er zijn wel aanwijzingen dat bepaalde vormen van datagedreven politiewerk kunnen bijdragen aan de effectiviteit van politiewerk, maar het doen van onderbouwde uitspraken is op dit moment niet mogelijk. De effectiviteit van datagedreven politiewerk is vooralsnog dus vooral een veronderstelde effectiviteit: *meer een potentie dan een vastgestelde realiteit*. De aanname van effectiviteit is gebaseerd op de eerdergenoemde uitbreiding of versterking van de vermogens van de politie tot waarnemen en informatie verwerken. Het is waarschijnlijk dat deze versterkte vermogens van de politie *leiden tot meer effectiviteit* in termen van het voorkomen, detecteren, tegenhouden en ophelderen van criminaliteit. Of de potentie van datagedreven politiewerk wordt waargemaakt, is afhankelijk van veel meer dan de (door)ontwikkeling van technologie. De effectiviteit van datagedreven politiewerk wordt uiteindelijk bepaald door het optreden of handelen van de politie in al diens verschijningsvormen. Effectiever (willen) zijn, veronderstelt veelal anders handelen dan voorheen. Accurate voorspellingen van waar criminaliteit gaat plaatsvinden, leiden alleen tot preventie als de politie iets anders doet dan het meegeven van een surveillanceopdracht aan een al belaste noodhulpeenheid. Beter inzicht in het veiligheidsprobleem is alleen waardevol als de politie iets anders doet dan op incidentgerichte wijze, van elkaar 'losstaande', opsporingsonderzoeken uitvoeren. Bulkdata en 'bewijs zoekt zaak' zijn alleen effectiever als de politie gericht met het al aanwezige bewijs aan de slag gaat in plaats van opnieuw begint met verzamelen. Snelle beschikbaarheid van uitkomsten van DNA-onderzoek is alleen effectiever als de politie het ook gebruikt in de beginfase van het opsporingsonderzoek. Et cetera. Meer data en geavanceerdere analyses leiden niet vanzelf tot andere of betere maatschappelijke opbrengsten van politiewerk. Er is vaak (te) veel hoop of optimisme ten aanzien van wat datagedreven politiewerk kan brengen.[3] Dit optimisme houdt (onder andere) te weinig rekening met het gegeven dat technologie niet deterministisch is. Technologie kan bijdragen aan vernieuwing in politiewerk, maar het dwingt die vernieuwing niet af. Vernieuwing in politiewerk komt tot stand in sociaal-technologische configuraties. In deze con-

3 Onder dit optimisme ligt een geloof dat in de literatuur *dataïsme* wordt genoemd: de overtuiging dat we via dataficatie, grootschalige dataverzameling en geavanceerde analyse tot geoptimaliseerde kennis en controle kunnen komen (zie Rasch 2020; zie ook Harari 2017). Dit dataïsme is ook binnen de politie aanwezig.

figuraties zijn sociale praktijken doorslaggevend. In iedere fase – van implementatie tot het gebruik in de operatie – zijn het sociale processen en verhoudingen die hun stempel drukken. Om die reden moeten technologische innovatie en sociale innovatie – anders kijken, anders denken en anders doen – *hand in hand gaan* om de potentie van datagedreven politiewerk waar te maken.

12. De potentie van datagedreven politiewerk heeft ook een keerzijde: de uitbreiding van het vermogen tot waarnemen en gegevens verwerken, gaat gepaard met risico's voor mensenrechten en de rechtsstaat. Het eerste risico bestaat uit toenemende inbreuken op de persoonlijke levenssfeer (privacy) van burgers. Door het gebruik van opkomende technologieën in het politiewerk *nemen de omvang en diepgang van surveillance toe*: over steeds meer burgers worden steeds meer gegevens vergaard, die worden opgeslagen, gecombineerd en geanalyseerd en zodoende ook steeds meer inzicht in het leven van burgers geven. Dit heeft als gevolg dat er *sneller een meer dan geringe inbreuk* op de persoonlijke levenssfeer van zowel verdachte als onverdachte burgers wordt gemaakt. De regulering van de gegevensverzameling en -verwerking door de politie hobbelt achter de praktijk aan. Dit is voor de politie vervelend, omdat niet altijd duidelijk is welke mogelijkheden zij (niet) mag benutten, maar het is vooral een probleem voor burgers die te maken hebben met een (soms forse) inbreuk op hun privacy. Het gaat dan in het bijzonder om onverdachte burgers, die door de politie en haar partners als risicovol worden getaxeerd met meer surveillance en eventueel proactief optreden tot gevolg. Een bijkomend probleem is dat de burger die als risicovol wordt getaxeerd en met (een vorm van) meer intensieve politiebemoeienis te maken krijgt weinig (rechts)bescherming geniet.
13. Daarnaast bestaat het risico dat de meer diepgaande surveillance zich vooral richt op burgers in kwetsbare omstandigheden, in het bijzonder burgers met een migratieachtergrond. Dit wordt onder andere veroorzaakt door verschillende vormen van vertekening (bias) in de data die worden gebruikt om tot risicotaxatie te komen. Deze vormen van vertekening kunnen er gezamenlijk toe leiden dat burgers met een migratieachtergrond *vaker onterecht als risicovol worden aangemerkt* dan burgers met een Nederlandse achtergrond. Anders gezegd: burgers met een migratieachtergrond worden vaker onterecht lastiggevallen (valpositief), terwijl burgers met een Nederlandse achtergrond een grotere kans hebben om onterecht met rust te worden gelaten (valsnegatief). De onvermijdelijke imperfectie van risicotaxatie heeft vermoedelijk dus vooral voor burgers met een migratieachtergrond nadelige consequenties, in het bijzonder wanneer repressie op risicotaxatie volgt. Het gezicht van de politie wordt voor hen dan grimmiger.[4] Dit doet onder andere afbreuk aan het streven naar het zijn van een politie voor iedereen.
14. De risico's van datagedreven politiewerk hebben niet alleen te maken met mensenrechten, maar ook met *de verhoudingen in de rechtsstaat*. De scheiding van de wetgevende, rechterlijke en uitvoerende macht komt onder druk te staan, omdat de politie – als uitvoerende macht – het meest machtig is. Zij heeft de data, de exper-

4 Deze formulering leen ik van Frissen 2022.

tise en ontwerpt de technologie of koopt die in. De wetgevende macht loopt achter de feiten aan en de rechterlijke macht komt pas in beeld als iemand daar werk van maakt. Er is dus onvoldoende (democratische) controle. Hierbij komt dat (zelflerende) algoritmen om verschillende redenen nauwelijks transparant – en daarmee moeilijk controleerbaar zijn. Op dit moment ligt de verantwoordelijkheid om ervoor te zorgen dat het gebruik van opkomende technologieën in het politiewerk op verantwoorde wijze plaatsvindt vooral bij de politie. Er is – naar mijn idee – geen reden om de politie bij voorbaat te wantrouwen in de wijze waarop met deze verantwoordelijkheid wordt omgegaan. De politie investeert inmiddels ook behoorlijk in waarborgen om op verantwoorde wijze met opkomende technologieën om te (kunnen) gaan. Dit neemt echter niet weg dat het in een rechtsstaat simpelweg *te kwetsbaar* is. Het ontbreekt aan tegenkracht. De maatregelen die worden genomen om die tegenkracht te organiseren, zijn te veel gebaseerd op oude methoden die niet goed aansluiten bij de nieuwe werkelijkheid en zijn daarnaast – weliswaar in afnemende mate – te vrijblijvend en reactief.

15. De optelsom van de drie hiervoor genoemde punten is dat datagedreven politiewerk een bedreiging kan zijn voor de normatieve legitimiteit van de politie. De normatieve legitimiteit is gebaseerd op de fundamentele beginselen en waarden die zijn verbonden aan de democratische rechtsstaat.[5] Het missiestatement van de politie is 'waakzaam en dienstbaar aan de waarden van de rechtsstaat', maar de politie moet naar mijn idee oppassen dat het gebruik van opkomende technologieën ten behoeve van waakzaamheid en dienstbaarheid niet leidt tot politiepraktijken die de waarden van de rechtsstaat juist *ondermijnen*.[6] De legitimiteit van de politie in Nederland is echter niet alleen gebaseerd op het perspectief van de rechtsstaat, maar ook op het perspectief van burgers: vinden burgers het optreden van de politie rechtvaardig en wordt dit optreden door burgers geaccepteerd? Dit is de sociale legitimiteit. De (mogelijke) gevolgen van het gebruik van opkomende technologieën voor de sociale legitimiteit van de politie zijn vooralsnog minder duidelijk dan die voor de normatieve legitimiteit. We weten op dit moment weinig over hoe burgers aankijken tegen de ontwikkelingen die in de afgelopen jaren binnen de politie in gang zijn gezet.[7] Wel kan worden vastgesteld dat de ontwikkelingen die in dit boek zijn beschreven onvermijdelijk bijdragen aan het *abstracter worden* van de politie. Dit wil zeggen dat de relaties binnen de politieorganisatie én tussen de politie en 'de' burger een meer afstandelijk, onpersoonlijk karakter krijgen.[8] Datagedreven politiewerk leidt op verschillende manieren tot een meer abstracte po-

5 Terpstra 2010a.

6 Zie ook Friedman 2017.

7 Een uitzondering is het kwalitatieve onderzoek dat in opdracht van de politie door het Rathenau Instituut is uitgevoerd naar de inzet van sensor-toepassingen (zie Snijders et al. 2019). Hieruit komt naar voren dat burgers niet bij voorbaat tegen of voor een bepaalde (sensing)technologie zijn. Hun houding is vooral afhankelijk van de specifieke omstandigheden waarin technologie wordt ingezet. Hoe onveiliger een situatie wordt ingeschat, hoe meer geoorloofd men de inzet van (sensing)technologie vindt. Hierbij moet worden voldaan aan randvoorwaarden op het gebied van onder andere privacy en persoonlijke vrijheid.

8 Terpstra, Fyfe & Salet 2019.

litieorganisatie. De toenemende automatisering van het vermogen tot waarnemen en informatie verwerken heeft tot gevolg dat een deel van de menselijkheid uit de politieorganisatie verdwijnt.[9] Er ontstaan in het politiewerk – zoals gezegd – betekenisgevers zonder hersens en zonder lichaam. Hierdoor wordt de betekenisgeving abstracter van aard: burgers worden vooral bekeken (als object) in plaats van gezien (van mens tot mens). 'Wie een rekensom op menselijke levensgangen loslaat, slaat dergelijke levens plat.'[10] De beschreven ontwikkelingen leiden er daarnaast toe dat het politiewerk vanuit het perspectief van de samenleving onzichtbaarder wordt. Niet alleen vanwege de overname van bepaalde activiteiten door technologie, maar ook doordat het politiewerk meer achter het bureau plaatsvindt en meer lokaal 'ont-bed' raakt. Kortom: als het politiemodel van datagedreven politiewerk dominanter wordt en andere politiemodellen meer naar de achtergrond bewegen, dan heeft dit een meer abstracte politie tot gevolg. Een meer abstracte politie kan leiden tot *afnemend vertrouwen* van (bepaalde, meer kwetsbare, groepen) burgers in de politie en daarmee afbreuk doen aan de sociale legitimiteit van de politie.

Op basis van deze vijftien punten keer ik terug naar de vraag waarmee dit boek is begonnen: hoe wezenlijk of fundamenteel zijn de veranderingen die in het politiewerk gaande en aanstaande zijn? De politie heef zelf als stelling dat de kern van het politiewerk tijdloos is.[11] Hiermee wordt verwezen naar de opdracht van de politie: de politie is waakzaam en dienstbaar aan de waarden van de rechtsstaat door – afhankelijk van de situatie – te beschermen, te begrenzen en te bekrachtigen. Er is veel voor te zeggen dat deze kern van het politiewerk en de formele taken van de politie inderdaad een relatief tijdloos karakter hebben.[12] Deze verkenning geeft in ieder geval geen aanleiding om te veronderstellen dat er op dit abstractieniveau iets is veranderd of op korte termijn gaat veranderen. De veranderingen die in het politiewerk gaande en aanstaande zijn, hebben vooral betrekking op *de wijze waarop* het politiewerk *binnen* de tijdloze kern wordt uitgevoerd. De derde industriële revolutie heeft in het politiewerk in essentie geleid tot twee gevolgen: het veiligheidsvraagstuk is – zoals aangegeven – gedigitaliseerd en de politie is ICT gaan gebruiken om het politiewerk te ondersteunen. De veranderingen die in het afgelopen tien of vijftien jaar in het politiewerk hebben plaatsgevonden, zijn naar mijn indruk meer veroorzaakt door de digitalisering van het veiligheidsvraagstuk dan door het gebruik van ICT in het politiewerk, al hangen beide vanzelfsprekend ook samen. De vierde industriële revolutie lijkt tot een omgekeerd patroon te leiden. Het veiligheidsvraagstuk zal verder digitaliseren en de politie zal met

9 Zie ook De Kool, Vermeeren & Steijn (2023) over het risico van het digitale contact tussen politie en samenleving.
10 Schnitzler 2021: 70.
11 Zie bijvoorbeeld Politie 2022.
12 Al kan het belang dat door de tijd heen aan bepaalde taken wordt gehecht wel veranderen. Denk aan de nadruk die nu ligt op bewaken en beveiligen, wat aanleiding is geweest om dit in 2022 te benoemen als een hoofdtaak van de politie.

nieuwe fenomenen en meer technologisch geavanceerde *modus operandi* te maken krijgen, maar de kern van de *crime change* heeft in de afgelopen twee decennia al plaatsgevonden. Het gebruik van opkomende technologieën in het politiewerk in het algemeen en AI in het bijzonder zal (zeer waarschijnlijk) in de komende periode *de voornaamste drijver van verandering* in politiewerk zijn. Het begin van deze veranderingen is nu zichtbaar, maar ik vermoed dat het nog vijf tot tien jaar duurt voordat deze veranderingen in (min of meer) de volle breedte van het politiewerk zichtbaar zijn.

De vraag is echter hoe we deze (verwachte) ontwikkeling moeten waarderen. Deze verkenning maakt duidelijk dat de potentie van datagedreven politiewerk net zo waarschijnlijk is als de risico's.[13] Het is een zegen en een vloek. Het is maar waar je de nadruk op wilt leggen. Maxim Februari formuleert het naar mijn mening treffend: 'Je hebt verschillende taalregisters tot je beschikking, verschillende stijlen waarmee je duidelijk kunt maken hoe je aankijkt tegen technologie die de toekomst vormgeeft.'[14] Ik wantrouw de jubelverhalen én de dystopische voorspellingen. Ze zijn meeslepend, maar missen precisie. Precisie is nodig omdat zowel de potentie als de risico's tussen de verschillende technologische toepassingen in het politiewerk (fors) kunnen verschillen. Het is niet wenselijk om alles op één hoop te gooien. De verhouding tussen potentie en risico is situationeel.[15] In algemene zin geldt wel dat de verdere ontwikkeling van datagedreven politiewerk – vanwege diens risico's – om politieke afwegingen vraagt.[16] Er moeten belangen worden afgewogen.

> *'Even with eyes wide open, goodwill, competent agents, and best practices, the surveillance actions taken (or not taken) may have multiple consequences for legitimate values and interests–serving some while undermining others… We can't have it all; repasts always cost someone something, somewhere, sometime.'*[17]

Het gaat uiteindelijk om de vraag wat voor een politie we in Nederland willen hebben. Zorgvuldigheid bij de ontwikkeling naar datagedreven politiewerk is daarom van groot belang. Ik sluit mij vanuit dit perspectief aan bij een suggestie van Sarah Brayne in haar studie naar datagedreven politiewerk door het LAPD: *slow down*.[18] Vertragen klinkt misschien weinig aantrekkelijk voor een politieorganisatie die het gevoel heeft diens been te moeten bijtrekken voor wat betreft digitalisering en opkomende technologieën,[19] maar is toch verstandig met het oog op het vooraf doordenken van de effecten van voorgenomen praktijken. Kees Verhoeven noemt dit *functioneel* vertragen.[20]

13 Ferguson 2017a.
14 Februari 2023: 7.
15 Marx 2016.
16 Hierbij sluit ik aan bij de meer algemene notie van Susskind (2022) die betoogt dat we politieker over technologie moeten gaan denken.
17 Marx 2016: 299.
18 Brayne 2021.
19 Egbert & Leese 2021.
20 Verhoeven 2023.

De tijd die je neemt, moet je dus wel goed benutten. Dat brengt me bij de laatste paragraaf van dit boek over wetenschappelijk onderzoek: we moeten meer leren over de (onbedoelde) gevolgen van datagedreven politiewerk voor zowel samenleving als politie(mensen). Ik citeer nogmaals Gary Marx, omdat hij het zo mooi formuleert:

> *'Making surveillance (and any technology) more visible and understandable hardly guarantees a just and accountable democratic society, but it is surely a necessary condition for one.'* [21]

Tussen beschouwen en onderzoeken

Dit boek is een geïnformeerde beschouwing over technologie, criminaliteit en politiewerk (zie hoofdstuk 1). Om de beschouwing te 'informeren', heb ik gebruikgemaakt van zo veel mogelijk relevante publicaties. Kenmerkend voor deze publicaties is dat het overgrote deel geen empirisch karakter heeft.[22] Het empirisch onderzoek dat wel is verricht, komt in de regel uit andere landen dan Nederland. Er doet zich dan ook een opmerkelijke discrepantie voor tussen enerzijds het belang dat wordt toegekend aan datagedreven politiewerk en anderzijds de geringe hoeveelheid en het eenzijdige – op predictive policing georiënteerde – karakter van empirisch onderzoek dat naar praktijken van datagedreven politiewerk is uitgevoerd.[23]

Meer onderzoek in Nederland is noodzakelijk om besluitvorming over de (verdere) ontwikkeling van datagedreven politiewerk te ondersteunen. Met betrekking tot dit onderzoek zijn in ieder geval de volgende punten van belang:

- Een brede invalshoek. Datagedreven politiewerk is veel meer dan predictive policing en de verschijningsvorm predictive mapping. Dit betekent dat ook empirisch onderzoek naar andere toepassingen van datagedreven politiewerk moet worden verricht, zodat recht wordt gedaan aan de veelzijdige werkelijkheid die schuilgaat achter datagedreven politiewerk.[24]
- Een empirisch karakter. Er is op dit moment vooral behoefte aan onderzoek naar datagedreven politiewerk als praktijk.[25] Het gaat dan om (gedetailleerde) beschrijvingen van hoe technologie in het politiewerk wordt gebruikt en tot welke effecten het leidt in zowel de politieorganisatie als de samenleving.[26] Hieronder vallen ook pogingen om de effectiviteitsvraag te beantwoorden.
- Een holistische aanpak. In onderzoek naar datagedreven politiewerk moet oog zijn voor zowel technologische als sociale processen (en het samenspel hiertussen).[27] Dit impliceert tevens dat onderzoekers of onderzoeksteams moeten beschikken

21 Marx 2016: 320.
22 Zie ook De Kool, Vermeeren & Steijn 2023.
23 Zie ook Egbert & Leese 2021; Terpstra & Salet 2020.
24 McDaniel & Pease 2021a; zie ook Marx 2016.
25 Terpstra & Salet 2020.
26 De Pauw 2019; McDaniel & Pease 2021a.
27 Waardenburg 2021.

over verschillende expertisegebieden. Ook van oorsprong sociaal-wetenschappelijke onderzoekers moeten tot op zekere hoogte 'digitaal fit' zijn en opkomende technologieën op een basisniveau begrijpen.

Ik hoop dat dit boek heeft bijgedragen aan een eerste overzicht van het gebruik van opkomende technologieën door de politie en de (mogelijke) gevolgen van dit gebruik voor zowel de politie als de samenleving. Het is nu van belang om van overzicht naar meer inzicht te komen. Dit inzicht is nodig omdat het in essentie gaat over hoe politiewerk in de samenleving vorm krijgt: wat voor een politie willen we in onze samenleving hebben? Daarover moeten we – politiemensen, gezagsdragers, bestuurders, politici, wetenschappers en burgers – met elkaar in gesprek. Het is er belangrijk genoeg voor.

Literatuurlijst

Adang, O., B. Mali & K. Vermeulen (2022). *Geweldig of gevaarlijk? Het stroomstootwapen in de basispolitiezorg*. Boom Criminologie.

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

Adjiembaks, S., A.H. Boer & M.J. Oude Lansink (2022). *(On)zichtbare beelden van jonge aanwas in de drugscriminaliteit. Een meta-analyse van tien deelonderzoeken in de regio Midden-Nederland*. RIEC Midden-Nederland/ESSA Research.

Adviescommissie Landelijke Eenheid (2022). *Ruimte voor slagvaardig politiewerk. Eindadvies van de Adviescommissie voor de Landelijke Eenheid*.

Agrawal, A., J. Gans & A. Goldfarb (2022). *Power and prediction. The disruptive economics of artificial intelligence*. Harvard Business Review Press.

Akkermans, M.M.P., R. Kloosterman, E. Moons, C. Reep & M. Tummers-van der Aa (2022). *Veiligheidsmonitor 2021*. Centraal Bureau voor de Statistiek/Ministerie van Justitie en Veiligheid.

Akkermans, M.M.P., J. Arends, E. Derksen & C. Reep (2023). *Online veiligheid en criminaliteit 2022*. Centraal Bureau voor de Statistiek.

Algemene Inlichtingen- en Veiligheidsdienst (2023). *AI-systemen: ontwikkel ze veilig*. AIVD.

Algemene Rekenkamer (2022). *Algoritmes getoetst. De inzet van 9 algoritmes bij de overheid*. Algemene Rekenkamer.

Almeida, D., K. Shmarko & E. Lomas (2022). '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*, 2, p. 377-387.

Amnesty International (2020). *We sense trouble. Automated discrimination and mass surveillance in predictive policing in the Netherlands*. Amnesty International.

Amnesty International (2021). *Xenophobic machines. Discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal*. Amnesty International.

Amnesty International (2023). *Ongecontroleerde macht. ID-controles en gegevensverzameling van vreedzame demonstranten in Nederland*. Amnesty International.

Antonopoulos, G.A. & G. Papanicolaou (2018). *Organized crime. A very short introduction*. Oxford University Press.

Arentze, L., D. Dekkers, P. Sinning, F. Bekkers & T. Sweijs (2023). *De staat van de rechtsstaat. Waar staan we? Waar gaan we naartoe?* The Hague Centre for Strategic Studies.

Arets, M. (2020). *Platformrevolutie. Van Amazon tot Zalando, de impact van platformen op hoe wij werken en leven*. Management Impact.
Ariel, B. (2019). 'Technology in policing: advocate'. In: D. Weisburd & A.A. Braga (Eds.), *Police innovation. Contrasting perspectives* (p. 485-515). Cambridge University Press.
Aslander, M., A. Broere & M. Meinema (2022). *Ons werk is stuk. Tips en inzichten voor onderhoud en reparatie*. Uitgeverij Publiek Denken BV.
Autoriteit Persoonsgegevens (2020). *Belastingdienst/Toeslagen. De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag*. AP.
Autoriteit Persoonsgegevens (2021). *Smart cities. Onderzoeksrapport bescherming van persoonsgegevens in de ontwikkeling van Nederlandse smart cities*. AP.
Autoriteit Persoonsgegevens (2023). *Rapportage algoritmerisico's Nederland. Periodiek inzicht in risico's en effecten van de inzet van algoritmes in Nederland*. AP.
Ávila, F., K. Hannah-Moffat & P. Maurutto (2021). 'The seductiveness of fairness: Is machine learning the Answer? Algorithmic fairness in criminal justice systems'. In: M.B. Schuilenburg & R. Peeters (Eds.), *The algorithmic society. Technology, power and knowledge* (p. 87-103). Routledge.

Bacon, M. (2016). *Taking care of business. Police detectives, drug law enforcement and proactive investigation*. Oxford University Press.
Balko, B. (2013). *Rise of the warrior cop. The militarization of America's police forces*. PublicAffairs.
Ball, M. (2022). *The Metaverse. And how it will revolutionize everything*. Liveright Publishing Corporation.
Bantema, W., J. Kerstens, S. Veenstra, S. Westers & W.P. Stol (2018). *Automatic number plate recognition (ANPR). Een studie naar effecten in politiewerk*. NHL Stenden Hogeschool/Politieacademie.
Bantema, W., S. Westers, M. Hoekstra, R. Herregods & S. Munneke (2021). *Black box van gemeentelijke online monitoring. Een wankel fundament onder een stevige praktijk*. Sdu Uitgevers.
Baricco, A. (2018). *The game*. De Bezige Bij.
Barros, A.I. (2022). *De kracht van intelligence: bezint eer ge moet bijsturen*. Politieacademie.
Barros, A.I., B.M.J. Keijser, K. van der Zwet & S. Wemmers (2022). 'Being two steps ahead: the added value of anticipatory intelligence analysis in law enforcement'. In: G. Adlakha-Hutcheon & A. Masys (Eds), *Disruption, ideation and innovation for defence and security. Advanced sciences and technologies for security applications* (p. 243-266). Springer.
Bas Seyyar, M. & Z.J.M.H. Geradts (2020). 'Privacy impact assessment in large-scale digital forensic investigations'. *Forensic Science International: Digital Investigation*, 33, p. 1-9.

Bastrup-Birk, J., E. Frinking, L. Arentze, E. de Jong & F. Bekkers (2023). *Next generation organised crime. Systemic change and the evolving character of the transnational organised crime*. The Hague Centre for Strategic Studies.
Bayley, D. (1994). *Police for the future*. Oxford University Press.
Beaulieu, A. & S. Leonelli (2022). *Data and society. A critical introduction*. Sage Publications.
Beerthuizen, M.G.C.J., T. Sipma & A.M. van der Laan (2020). *Aard en omvang van dader- en slachtofferschap van cyber- en gedigitaliseerde criminaliteit in Nederland*. Wetenschappelijk Onderzoek- en Documentatiecentrum.
Bekkers, F., E. de Jong, L. Jasper & E. MacLaughlin (2023). *Maatschappelijke ontgoocheling van de middenklasse. Optreden, oorzaken en gevolgen*. The Hague Centre for Strategic Studies.
Bekkers, L., Y, van Houten, R. Spithoven & E.R. Leukfeldt (2023). 'Money mules and cybercrime involvement mechanisms: exploring the experiences and perceptions of young people in the Netherlands'. *Deviant Behavior*. DOI: 10.1080/01639625.2023.2196365 .
Benschop, C.G., M. Slagter, S. Smit & A.L.J. Kneppers (2022). 'Automated DNA casework workflow: a retrospective study of the first implementation of FIDL at the Netherlands Forensic Institute'. *Forensic Science International: Genetics Supplement Series*, 8, p. 257-258.
Berends, I. & M. Kempes (2015). *Overeenkomst en voorspellende waarde van risicotaxatie van geweldsrecidive in verschillende fasen van de jeugdstrafrechtsketen*. Nederlands Instituut voor Forensische Psychiatrie en Psychologie.
Bergdahl, J. (2020). *This is real AI. 100 real-world implementations of artificial intelligence*. Independently Published.
Berk, R.A. (2021). 'Artificial intelligence, predictive policing, and risk assessment for law enforcement'. *Annual Review of Criminology*, 4, p. 209-237.
Berkel, J.J. van, C.A.J. van den Eeden & C.J. de Poot (2020). *Het gebruik van bewaarde kentekengegevens in de opsporing. De wet 'vastleggen en bewaren van kentekengegevens door de politie' een jaar in werking*. Wetenschappelijk Onderzoek- en Documentatiecentrum.
Berkel, J.J. van, R.L.D. Pool, M. Harbers, J.J. Oerlemans, M.S. Bargh & S.W. van den Braak (2017). *(Verkeerd) verbonden in een slimme samenleving. Het Internet of Things: kansen, bedreigingen en maatregelen*. Wetenschappelijk Onderzoek- en Documentatiecentrum.
Berkel, J.J. van, A. van Uden & C.J. de Poot (2021). *Evaluatie ANPR-wetgeving 126jj Wetboek van Strafvordering. De wet 'vastleggen en bewaren van kentekengegevens door de politie' geëvalueerd*. Wetenschappelijk Onderzoek- en Documentatiecentrum.
Bervoets, E., M. Corsel, G. Fortuin, K. Kaal & M. van de Ven (2021). *Doorbraak verzocht. Onderzoek naar kwetsbaarheden voor crimineel misbruik en (publiek-private) maatregelen in het beroepsgoederenvervoer over de weg*. Van de Ven.
Beugelsdijk, S. (2021). *De verdeelde Nederlanden. Hoe een perfecte storm een klein land dreigt te splijten (en wat we daaraan kunnen doen)*. Uitgeverij Balans.

Beurskens, E., M. van der Linde & A. Baart (2019). *Praktijkboek presentie*. Uitgeverij Countinho.
Bex, F. & H. Prakken (2020). De juridische voorspelindustrie: onzinnige hype of nuttige ontwikkeling? *Ars Aequi*, *69*(3), p. 255-259.
Bezemer, W. & A. Leerkes (2021). *Oververtegenwoordiging verder ontcijferd. Een kwantitatief onderzoek naar sociale verschillen in verdenkingskans en zelfgerapporteerd crimineel gedrag onder jongeren in Nederland*. Sdu Uitgevers.
Bichler, G. (2019). *Understanding criminal networks. A research guide*. University of California Press.
Bichler, G. & A. Malm (2019). 'Social network analysis'. In: R. Wortley, A. Sidebottom, N. Tilley & G. Laycock (Eds.), *Routledge handbook of crime science* (p. 207-222). Routledge.
Bijlsma, J., F. Bex & G. Meynen (2019). Artificiële intelligentie en risicotaxatie. Drie kernvragen voor strafrechtjuristen. *Nederlands Juristenblad*, 44, p. 3313-3319.
Bird, L., T. Hoang, J. Stanyard, S. Walker & S. Haysom (2020). *Transformative technologies. How digital is changing the landscape of organized crim*e. Global Initiative Against Transnational Organized Crime.
Bittner, E. (1970). *The functions of the police in modern society. A review of background factors, current practices and possible role models*. Oelgeschlager, Gunn & Hain.
Bland, M. (2020). '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* (p. 139-156). Springer.
Bland, M. (2022). 'Why every crime analyst needs a companion'. In: M. Bland, B. Ariel & N. Ridgeon (Eds.), *The crime analyst's companion* (pp. 1-12). Springer.
Block, L. (2023). The long history of OSINT. *Journal of Intelligence History*. DOI: 10.1080/16161262.2023.2224091.
Blythe, J.M. & S.D. Johnson (2021). 'A systematic review of crime facilitated by the consumer Internet of Things'. *Security Journal*, 34, p. 97-125.
Boba Santos, R. (2019). 'Critic. Predictive Policing: where's the evidence'. In: D. Weisburd & A.A. Braga (Eds.), *Police innovation. Contrasting perspectives* (p. 366-396). Cambridge University Press.
Boden, M. (2018). *Artificial Intelligence. A very short introduction*. Oxford University Press.
Boekhoorn, P. (2019). *De aanpak van cybercrime door regionale eenheden van de politie. Van intake van cybercrime naar opsporing en vervolging*. Sdu Uitgevers.
Boelens, M. & W. Landman (2021). *Pionieren in gebiedsgebonden politiewerk. Een onderzoek naar de digitaal wijkagent*. Politie Nederland/Twynstra Gudde.
Boer, H. de, H. Ferwerda & J. Kuppens (2022). *Do or don't. Kennissynthese ingroeimechanismen en rekruteringsprocessen van jongeren in de georganiseerde criminaliteit*. WODC/Bureau Beke.
Boeser, J.S. (2021). 'Cybersecurity en "datagedreven" opsporing: stand van zaken met betrekking tot de interceptie van versleutelde cryptocommunicatie'. *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 5, p. 351-356.

Boïng, B. (2013). 'Professional disobedience. The impact of technology and multilevel dispatching on police practice'. *European Journal of Policing Studies*, *1*(2), p. 91-109.
Böing, B. & P. de Vries (2021). 'De inzet van Virtual Reality bij het tegengaan van etnisch profileren'. *Het Tijdschrift voor de Politie*, 4, p. 28-34.
Borek, A. & N. Prill (2020). *Driving digital transformation through data and AI. A practical guide to delivering data science and machine learning products*. KoganPage.
Borking, J.J.F.M. (2010). *Privacyrecht is code. Over het gebruik van Privacy Enhancing Technologies*. Kluwer.
Bouteca, N., T. Leys, J. Pohlmann, K. Segers, D. Deweer, J. Malcorps & J. de Bruyne (2020). 'AI en ideologie'. In: J. de Bruyne & N. Bouteca (Red.), *Artificiële intelligentie en maatschappij* (pp. 49-74). Gompel&Svacina.
Boutellier, H. (2002). *De veiligheidsutopie. Hedendaags onbehagen en verlangen rondom misdaad en straf*. Boom Juridische Uitgevers.
Boutellier, H. (2019). 'Hoe veilig verder. Over wat niet deugt, wat je eraan kunt doen en wat je daar dan weer van moet denken'. In: R. van Steden & R. van Putten (Red.), *Pragmatisch verzet tegen cultuurpessimisme. In gesp ek met het oeuvre van Hans Boutellier* (p. 15-30). Boom Bestuurskunde.
Boutellier, H. (2020). *Politie! Over de kernfunctie van de politieorganisatie in de 21ste eeuw*. Politieacademie/Directie Strategie & Innovatie.
Boutellier, H. (2021). *Het nieuwe westen. De identitaire strijd om de sociale verbeelding*. Uitgeverij Van Gennep.
Boutellier, H., C. Hermans & F. van de Plas (2019). *Ontspoorde vrijheid. Over de betekenis van ondermijning en het belang van een onorthodoxe aanpak daarvan*. Boom Bestuurskunde.
Braga, A.A. & D. Weisburd (2019). 'Conclusion: politie innovation and the future of policing'. In: D. Weisburd & A.A. Braga (Eds.), *Police innovation. Contrasting perspectives* (p. 544-563). Cambridge University Press.
Brakel, R.E. van (2016). 'Pre-emptive big data surveillance and its (dis)empowering consequences: the case of predictive policing'. In: B. van der Sloot, D. Broeders & E. Schrijvers (Eds.), *Exploring the boundaries of big data* (p. 117-141). Amsterdam University Press.
Brakel, R.E. van (2021). 'Rethinking predictive policing. Towards a holistic framework of democratic algorithmic surveillance'. In: M.B. Schuilenburg & R. Peeters (Eds.), *The algorithmic society. Technology, power and knowledge* (p. 187-212). Routledge.
Brakel, R.E. van & P. de Hert (2011). 'Policing, surveillance and law in a pre-crime society: understanding the consequences of technology-based strategies'. In: E. de Pauw, P. Ponsaers, C.D. van der Vijver, W. Bruggeman & P. Deelman (Eds.), *Technology-led policing* (p. 163-192). Maklu Uitgevers.
Brayne, S. (2021). *Predict and surveil. Data, discretion, and the future of policing*. Oxford University Press.
Brink, G. van den (2020). *Ruw ontwaken uit een neoliberale droom en de eigenheid van het Europese Continent*. Prometheus.

Brink T. ten, J. ter Mors & M. de Hengst (2017). 'Informatiegestuurd werken en business intelligence'. In: M. den Hengst, T. ten Brink & J. ter Mors (Red.), *Informatiegestuurd politiewerk in de praktijk* (p. 21-36). Vakmedianet.
Brinkhoff, S. (2014). *Startinformatie in het strafproces*. Kluwer.
Brodeur, J-P. (2010). *The policing web*. Oxford University Press.
Broek, J. van den, I. van Elzakker, T. Maas & J. Deuten (2020). *Voorbij lokaal enthousiasme. Lessen voor de opschaling van living labs*. Rathenau Instituut.
Broek, J.B.A. van den, J. de Jong & Y. Moussaid (2022). *Handreiking rivaliserend groepsgedrag in een hybride werkelijkheid*. Partner in Crime.
Buitenweg, K. (2021). *Datamacht en tegenkracht. Hoe we de macht over onze gegevens kunnen terugkrijgen*. De Bezige Bij.
Burrington, I. (2016). *Networks of New York. An illustrated field guide to urban internet infrastructure*. Melville House.
Byrne, J. & G. Marx (2011). 'Technological innovations in crime prevention and policing. A review of the research of implementation and impact'. In: E. de Pauw, P. Ponsaers, C.D. van der Vijver, W. Bruggeman & P. Deelman (Eds.). *Technology-led policing* (p. 17-38). Maklu Uitgevers.

Cachet, L. (2019). 'Politiewerk. Over essenties in meervoud'. In: E. Devroe, A. Schmidt, L. Gunther Moor & P. Ponsaers (Eds.), *De essentie van politiewerk* (p. 225-230). Gompel & Svacina.
Cain, G. (2021). *The perfect police state. An undercover odyssey into China's terrifying surveillance dystopia of the future*. Public Affairs.
Caldwell, M., J.T.A. Andrews, T. Tanay & L.D. Griffin (2020). 'AI-enabled future crime'. *Crime Science*, 9, p. 1-14.
Campbell, C. (2022). *AI by design. A plan for living with artificial intelligence*. CRC Press.
Caneppele, S. & M.F. Aebi (2017). 'Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes'. *Policing*, *13*(1), p. 66-79.
Castells, M. (1996). *The rise of the network society*. Blackwell Publishing.
Castells, M. (1997). *Power of identity*. Blackwell Publishing.
Chan, J.B.L. (2001). 'The technological game. How information technology is transforming police practice'. *Criminal Justice*, *1*(2), p. 139-159.
Chouldevocha, A. (2017). 'Fair prediction with disparate impact. A study of bias in recidivism prediction instruments'. *Big data, 5*(2), p. 153-163.
Ciancaglini, V., C. Gibson, D. Sancho, O. McCarthy, M. Eira, P. Amann & A. Klayn (2020). *Malicious uses and abuses of artificial intelligence*. Trend Micro Research.
Cocking, D. & J. van den Hoven (2018). *Evil online*. Wiley Blackwell.
Coeckelbergh, M. (2020). *The political philosophy of AI. An introduction*. Polity Press.
Collier, B., D.R. Thomas, R. Clayton, A. Hutchings & Y. Ting Chua (2022). 'Influence, infrastructure and recentering cybercrime policing: evaluating emerging approaches

to online law enforcement through a market for cybercime services'. *Policing and Society*, 32(1), p. 103-124.
Commissie Evaluatie Politiewet 2012 (Commissie Kuijken) (2017). *Evaluatie Politiewet 2012. Doorontwikkelen en verbeteren*.
Commissie modernisering opsporingsonderzoek in het digitale tijdperk (Commissie Koops) (2018). *Regulering van opsporingsbevoegdheden in een digitale omgeving*.
Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (2021). *Automated OSINT: tools en bronnen voor openbronnenonderzoek*. CTIVD.
Cornish, D.B. (1994). The procedural analysis of offending and its relevance for situational crime prevention. In: R.V. Clarke (Eds.), *Crime prevention studies 3* (pp. 151-196). Criminal Justice Press.
Custers, B.H.M., J.J. Oerlemans & S.J. Vergouw (2015). *Het gebruik van drones. Een verkennend onderzoek naar onbemande luchtvaartuigen*. Wetenschappelijk Onderzoek- en Documentatiecentrum.

DalleMule, L. & Davenport, T.H. (2021). What's your data strategy? In: *HBR's 10 must reads on leading digital transformation*. Harvard Business Review Press.
Das, A. & M.B. Schuilenburg (2018). 'Predictive policing: waarom bestrijding van criminaliteit op basis van algoritmen vraagt om aanpassing van het strafprocesrecht'. *Strafblad*, 4, p. 19-26.
Daugherty, P.R. & H.J. Wilson (2018). *Human + machine. Reimagining work in the age of AI*. Harvard University Press.
Daugherty, P.R. & H.J. Wilson (2022). *Radically human. How technology is transforming business and shaping our future*. Harvard University Press.
Davenport, T.H. & N. Mittal (2023). *All in on AI. How smart companies win big with artificial intelligence*. Harvard University Press.
David, M. (2023). *Networked crime. Does the digital make a difference?* Bristol University Press.
Davies, P.K. (2002). *Analytic architecture for capabilities-based planning, mission-system analysis, and transformation*. Rand.
Dechesne, F., L. Zardiashvili, V. Dignum & J. Bieger (2019). *AI and ethics at the police. Towards responsible use of artificial intelligence in the Dutch police*. Leiden University/ TU Delft.
Degeling, M. & B. Berendt (2018). 'What is wrong about robocops as consultants? A technology-centric critique of predictive policing'. *AI & Society*, *33*(3), p. 347-356.
Deloitte (2020). *Hoe verder met het Programma Vernieuwend registreren*. Deloitte.
Denkers, F. (2001). 'Aspecten van het moreel kompas'. In: F. van Beers (Red), *Frans Denkers' Moreel Kompas van de politie* (p. 103-142). Den Haag: Koninklijke De Swart.
Devroe, E. (2017). 'Over toekomstbestendige policing. De dilemma's van veiligheidsregimes in grote steden'. *Justitiële Verkenningen*, *43*(4) p. 81-92.
Dewald, S. (2023). 'Detectives and technological frames. Integrating technology and social media into everyday work'. *Policing & Society*, *33*(1), p. 111-128.

Dijck, J. van, T. Poel & M. de Waal (2016). *De platformsamenleving. Strijd om publieke waarden in een online wereld*. Amsterdam University Press.
Diver, L.E. (2022). *Digisprudence. Code as law rebooted*. Edinburgh University Press.
Doorn M. van, S. Duivesteijn & T. Pepping (2021). *Echt nep. Spelen met de realiteit in tijden van AI, deepfakes en de Metaverse*. Bot Uitgevers.
Dressel, J.J. (2017). *Accuracy and racial biases of recidivism prediction instruments*. Dartmouth Computer Science Technical Report.
Dreżewskia, R., J. Sepielaka & W. Filipkowskib (2015). 'The application of social network analysis algorithms in a system supporting money laundering detection'. *Information Sciences-Informatics and Computer Science, Intelligent Systems, Applications: An International Journal*, *295*(C), p. 18-32.
Duijn, P.A.C. (2011). Intelligence en recherchestrategieën. In: N. Kop, R. van der Wal & G. Snel (Red.). *Opsporing belicht. Over strategieën in de opsporingspraktijk* (p. 63-94). Politieacademie.
Duijn, P.A.C. (2016). *Detecting and disrupting criminal networks. A data driven approach*. University of Amsterdam.
Duijn, P.A.C., V. Kashirin & P. Sloot (2014). 'The relative ineffectiveness of criminal network disruption'. *Scientific Report, 4*, p. 42-38.
Duursma, J. (2019). *Deepfake technologie. The infocalypse*. Studio Overmorgen.

Eckhouse, L., K. Lum, C. Conti-Cook & J. Ciccolini (2019). 'Layers of bias: a unified approach for understanding problems with risk assessment'. *Criminal Justice*, *46*(2), p. 185-209.
Edmondson, A.C. (2012). *Teaming. How organizations learn, innovate and compete in the knowledge economy*. John Wiley & Sons.
Eeden, C.A.J. van den, J.J. van Berkel, C.C. Lankhaar & C.J. de Poot (2021). *Opsporen, vervolgen en tegenhouden van cybercriminaliteit*. Wetenschappelijk Onderzoek- en Documentatiecentrum.
Eerste Kamer der Staten-Generaal (2022). *Gelijk recht doen. Deelrapport politie*. Eerste Kamer.
Egbert, S. & S. Krasmann (2020). 'Predictive policing: not yet, but soon preemptive?'. *Policing and Society*, *30*(8), p. 905-919.
Egbert, S. & M. Leese (2021). *Criminal futures. Predictive policing and everyday police work*. Routledge.
Egnoto, M., G. Ackerman, I. Iles, H.A. Roberts, A. Smith, B.F. Lui & B. Behlendorf (2017). 'What motivates the blue line for technology adoption? Insights from a police expert panel and survey'. *Policing: An International Journal of Police Strategies & Management*, *40*(2), p. 306-320.
Eijk, G. van (2021). 'Algorithmic reasoning. The production of subjectivity through data'. In: M.B. Schuilenburg & R. Peeters (Eds.). *The algorithmic society. Technology, power and knowledge* (p. 214-240). Routledge.

Ensign, D., S.A. Friedler, S. Neville, C. Scheidegger & S. Venkatasubramanian (2018). 'Decision making with limited feedback. Error bounds for predictive policing and recidivism prediction'. *Proceedings of Machine Learning Research, 83*, p. 1-9.
Ericson, R.V. & K.D. Haggerty (1997). *Policing the risk society*. University of Toronto Press.
Ernst, S. & N. Kop (2018). 'Zicht op technologische ontwikkelingen binnen de politie'. In: E. Devroe, L. Cachet, N. Kop & W. Bruggeman (Eds.), *Evaluatie van de politie* (p. 227-244). Gompel & Svacina.
Ernst, S., H. ter Veen, J. Lam & N. Kop (2019). *Leren van technologisch innoveren. 'De techniek is niet zo spannend'*. Politieacademie.
Eubanks, V. (2018). *Automating inequality. How high-tech tools profile, police, and punish the poor*. Picador.
Europol (2021a). European Union *serious and organised crime threat assessment. A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime*. Publications Office of the European Union.
Europol (2021b). *Europol Spotlight. The use of violence by organised crime groups*. Publications Office of the European Union.
Europol (2021c). *Europol Spotlight. Cryptocurrencies: tracing the evolution of criminal finances*. Publications Office of the European Union.
Europol (2022a). *Facing reality? Law enforcement and the challenge of deepfakes*. Publications Office of the European Union.
Europol (2022b). *Policing in the metaverse: what law enforcement needs to know. An Observatory Report from the Europol Innovation Lab*. Publications Office of the European Union.
Europol (2023a). ChatGPT. *The impact of large language models on law enforcement*. Europol Innovation Lab.
Europol (2023b). *Internet organised crime threat assessment 2023*. Publications Office of the European Union.
Eysink Smeets, M. (2022). *Onrust begrijpen begint bij anders kijken. Een veiligheidspsychologisch perspectief op maatschappelijke onrust*. Centrum voor Criminaliteitspreventie en Veiligheid.

Farrell, G., N. Tilley, A. Tseloni & J. Mailley (2010). 'Explaining and sustaining the crime drop: clarifying the role of opportunity-related theories'. *Crime prevention and communiy safety*, *12*(1), p. 24-41.
Farrall, S. (2017). *Re-examining the crime drop*. Palgrave Macmillan.
Februari, M. (2023). *Doe zelf normaal. Menselijk recht in tijden van datasturing en natuurgeweld*. Prometheus.
Fedorova, M.I., R.M. te Molder, M.J. Dubelaar, S.M.A. Lestrade & T.F. Walree (2022). *Strafvorderlijke gegevensverwerking. Een verkennende studie naar de relevante gezichtspunten bij de normering van het verwerken van persoonsgegevens voor strafvorderlijke doeleinden*. Radboud University Press.

Feenstra, M. (2018). 'Opsporingsmiddelen in ontwikkeling. Open-bronnenonderzoek als nieuwe "tap"'. *Proces*, 97(6), p. 367-375.
Ferguson, A.G. (2012). 'Predictive policing and reasonable suspicion'. *Emory Law Journal*, 62, p. 259-325.
Ferguson, A.G. (2017a). *The rise of big data policing. Surveillance, race, and the future of law enforcement*. New York University Press.
Ferguson, A.G. (2017b). 'Policing predictive policing'. *Washington University Law Review, 94*(5), p. 1109-1189.
Ferguson, A.G. (2017c). 'Predictive policing theory'. In: T.R. Lave & E.J. Miller (Eds.), *The Cambridge handbook of policing in the United States* (p. 491-510). Cambridge University Press.
Ferguson, A.G. (2020a). 'Facial recognition and the Fourth Amendment'. *Minnesota Law Review*, p. 101-206.
Ferguson, A.G. (2020b). 'Structural sensor surveillance'. *Iowa Law Review*, *106*, p. 47-112.
Ferguson, A.G. (2022). 'Why digital policing is different'. *Ohio State Law Journal*, p. 1-32.
Ferwerda, H., N. Brouwer, I. Hölzken & L. Kroese (2021). *Misdaadcarrières voorkomen en doorbreken. Van analyse van het netwerk naar aanpak*. Bureau Beke.
Fijnaut, C. (2021). 'Een criminologisch vergezicht op de zware misdaad in Nederland'. *Delikt en Delinkwent*, *48*(7), p. 620-635.
Fijnaut, C. (2023). *Over grenzen. Een leven tussen wetenschap, beleid en actie*. Prometheus.
Fiscale Inlichtingen- en Opsporingsdienst (FIOD) (2022). *Een duik in de NFT wereld. Een verkenning van techniek, gebruik en witwasrisico's*. FIOD.
Flight, S. (2017). *De mogelijke meerwaarde van bodycams voor politiewerk. Een internationaal literatuuronderzoek*. Reed Business.
Foster, D. (2023). *Generative deep learning. Teaching machines to paint, write, compose and play*. O'Reilly Media.
Foucault, M. (1989). *Discipline, Toezicht en Straf. De geboorte van de gevangenis*. Historische Uitgeverij Groningen.
Fountaine, T., B. McCarthy & T. Saleh (2021). 'Building the AI-powered organization'. *Harvard Business Review*, *97*(4), p. 62-73.
Franken, S. (2017). 'De Wpg'. In: M. den Hengst, T. ten Brink & J. ter Mors (Red.), *Informatiegestuurd politiewerk in de praktijk* (p. 65-85). Vakmedianet.
Friedman, B. (2017*). Unwarrented. Policing without permission*. Farrar, Straus and Giroux.
Frissen, P. (2022). *De volle plek van de macht. De versplinterde staat voorbij*. Tilburg University.
Fry, H. (2018). *Algoritmes aan de macht. Hoe blijf je menselijk in een geautomatiseerde wereld?* De Geus.
Fukuyama, F. (2019). *Identiteit. Waardigheid, ressentiment en identiteitspolitiek*. Uitgeverij Atlas Contact.

Fukuyama, F. (2022). *Het liberalisme en zijn schaduwzijden. Verdediging van een klassiek ideaal*. Uitgeverij Atlas Contact.

Galič, M. (2022). 'Bulkbevoegdheden en strafrechtelijk onderzoek Lessen uit de jurisprudentie van het EHRM voor de normering van grootschalige data-analyse'. *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 2, p. 130-137.
Ganesan, K. (2022). *The businesscase for AI. A leader's guide to AI strategies, best practices & real-world applications*. Opinosis Analytics Publishing.
Garland, D. (2001). *The culture of control. Crime and social disorder in contemporary society*. Oxford University Press.
Gelder, E. van (2022). *Het grote verwonderboek voor managers. Hoe sociale innovatie bijdraagt aan verandering en vernieuwing in jouw organisatie*. Van Duuren Management.
Gerritsen, J., J. Hamer, L. Kool & P. Verhoef (2020). 'Beter beschermd tegen biometrie'. *Beleid en Maatschappij*, *47*(4), p. 451-466.
Gestel, B. van (2021). 'Liquidaties en de verbreding van excessief geweld'. *Justitiële Verkenningen*, *47*(4), p. 9-22.
Gestel, B. van & M.A. Verhoeven (2017). 'Liquidaties nieuwe stijl. Verruwing en professionalisering bij liquidaties in Nederland'. *Justitiële Verkenningen*, 43(5), p. 9-28.
Giddens, A. (1990). *The consequences of modernity*. Polity Press.
Gigerenzer, G. (2022). *How to stay smart in a smart world. Why human intelligence still beats algorithms*. Penguin Books.
Goldstein, H. (1979). 'Improving policing. A problem-oriented approach'. *Crime & Delinquency*, 25(2): p. 236-258.
Goodman, M. (2015). *Future crimes. Inside the digital underground and the battle for our connected world*. Transworld Publishers.
Greenberg, A. (2022). *Tracers in the dark. The global hunt for the crime lords of cryptocurrency*. Doubleday.
Grimmelikhuijsen, S.G. (2022). 'Explaining why the computer says no. Algorithmic transparency effects the perceived trustworthiness of automated decision-making'. *Public Administration Review*, n/a(n/a). https://doi.org/10.1111/puar.13483.
Gruijter, M. de (2017). *The influence of rapid identification technologies on CSI behaviour*. Vrije Universiteit Amsterdam.
Gruijter, M. de, C. de Poot & H. Elffers (2016). 'Reconstructing with trace information: does rapid identification information lead to better crime reconstructions?'. *Journal of Investigative Psychology and Offender Profiling*, 14(1), p. 88-103.
Guilluy, C. (2019). *Twilight of the elites. Prosperity, the periphery, and the future of France*. Yale University Press.
Gundhus, H.O.I., P.E. Skjevrak & C.T. Wathne (2023). 'We will always be better than a spreadsheet. Intelligence logic and crime prevention in practice'. *European Journal of Policing Studies*, *6*(1), p. 27-49.

Haest, M. (2011). *De wijkagent. Bizarre buurtverhalen*. Uitgeverij Thomas Rap.

Hamilton, M. (2021). 'Predictive policing through risk assessment'. In: J.L.M. McDaniel & K.G. Pease (Eds.), *Predictive policing and artificial intelligence* (p. 58-78). Routledge.
Hanelt, A., R. Bohnsack, D. Marz & C.A. Marante (2022). 'A systematic review of the literature on digital transformation: insights and implications for strategy and organizational change'. *Journal of Management Studies*, *58*(5), p. 1159-1197.
Harari, Y.N. (2017). *Homo deus. Een kleine geschiedenis van de toekomst*. Thomas Rap.
Harcourt, B.E. (2007). *Against prediction. Profiling, policing and punishment in an actuarial age*. The University of Chicago Press.
Hayward, K.J. & M.M. Maas (2021). 'Artificial intelligence and crime: A primer for criminologists'. Crime, Media, Culture, *17*(2), p. 209-233.
Hazenberg, J. (2019). *Technologie de baas. Vooruitzichten en gevaren van de nieuwe industriële revolutie*. Spectrum.
Heijne, B. (2019). *Staat van Nederland. Een pleidooi*. Prometheus.
Helmus, T.C. (2022). *Artificial intelligence, deepfakes and disinformation. A primer*. RAND Corporation.
Hengst, M. den (2017). 'Keerpunt intelligence. Naar politiewerk in een informatiemaatschappij'. *Het Tijdschrift voor de Politie*, 79(6), p. 26-29.
Hengst, M. den, M. Bruinsma, Y. Schoenmakers & W. Niepce (2015). *Van intel tot operatie. De impact van veiligheidsanalisten bij de aanpak van misdaad*. Reed Business.
Hengst, M. den & O. Wijsman (2023). 'Datagedreven politiewerk. Een organisatorisch en juridisch perspectief'. In: T. Snaphaan, W. Hardyns, A. van Dijk, R. Spithoven & R. van Brakel (Eds.), *Big data policing* (p. 71-90). Gompel & Svacina.
Henseler, H. & C.J. de Poot (2020). 'De betekenis van digitale sporen voor bewijs op activiteitniveau'. *Expertise en Recht*, 2, p. 50-59.
Henseler, H. & H van Beek (2023). 'ChatGPT as a copolit for investigating digital evidence', *International Conference on Artificial Intelligence*, June 2023.
Hestehave, N.K. (2018). 'Predict crime? On challenges to the police in becoming knowledgeable organizations'. In: N.R. Fyfe, H.O.I. Gundhus & K.V. Rønn (Eds.), *Moral issues in intelligence-led policing* (p. 63-80). Routledge.
Higgins, E. (2021). *Wij zijn Bellingcat. Hoe gewone mensen de onderzoeksjournalisten van de toekomst werden*. Spectrum.
Hirsch Ballin, M.F.H. (2012). *Anticipative criminal investigation. Theory and counterterrorism practice in the Netherlands and the United States*. T.M.C. Asser Press.
Hirsch Ballin, M.F.H. & J.J. Oerlemans (2023). 'Datagedreven opsporing verzet de bakens in het toezicht op strafvorderlijk optreden'. *Delikt en Delinkwent*, 50(2), p. 18-38.
His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (2022). *Digital forensics. An inspection into how well the police and other agencies use digital forensics in their investigations*. Birmingham: HMICFRS.
Hodgers, D. (2021). 'Cyber-Enabled Burglary of Smart Homes'. *Computers & Security,* 110(3). https://doi.org/10.1016/j.cose.2021.102418.

Hoge Raad (2022). *Onderzoek in een geautomatiseerd werk. Over de toepassing van opsporingsbevoegdheden als bedoeld in de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1 van het Wetboek van Strafvordering door het Openbaar Ministerie*. Hoge Raad.
Holt, T.J., A.M. Bossler & K.C. Seigfried-Spellar (2022). *Cybercime and digital forensics. An introduction (third edition)*. Routledge.
Homburg, G., A. Schreijenberg, J. van den Tillaart & Y. Bleeke (2016). *ANPR: toepassingen en ontwikkelingen*. Regioplan.
Hoogenboom, A.B. (2009). *Bringing the police back in. Notes on the lost and found character of the police in police studies*. Stichting Maatschappij Veiligheid en Politie.
Hoorn, J. van (2011). 'Politiewerk in een kwetsbare samenleving'. *Het Tijdschrift voor de Politie*, 73(9), p. 6-10.
Hordijk, M. & T. Lindsen (2023). 'Kan de EU de black box openen? Een analyse van de Europese concept AI-verordening als toetsingskader voor de transparantie van AI-risicotaxatie in het licht van recidivevoorspelling'. In: C.J.H. Jansen (Red.), *Digitalisering en recht* (p. 85-100). Ars Aequi Libri.
House of Lords (2021). *Technology rules? The advent of new technologies in the justice system*. House of Lords.
Huijstee, M. van, W. Nieuwenhuizen, M. Sanders, E. Masson & P. van Boheemen (2021). *Online ontspoord. Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland*. Rathenau Instituut.
Hulst, R.C. van der (2008). 'Sociale netwerkanalyse en de bestrijding van criminaliteit en terrorisme'. *Justitiële Verkenningen,* 34(5), p. 10-32.
Hung, T-W. & C-P. Yen (2021). 'On the person-based predictive policing of AI'. *Ethics and Information Technology,* 23, p. 165-176.

Iansiti, M. & K.R. Lakhani (2020). *Competing in the age of AI. Strategy and leadership when algorithms and networks run the world*. Harvard University Press.
Inspectie Justitie & Veiligheid (2022). *Verslag toezicht wettelijke hackbevoegdheid politie 2021*. Inspectie J&V.
Interpol/UNICRI (2019). *Artificial intelligence and robotics for law enforcement*. Unicri/Interpol.
Ipenburg, D.C. (2023). 'Tussen plan en aanpak. Over het wetsvoorstel Wet plan van aanpak witwassen'. *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, *1*, p. 25-31.

Jansen, F. (2022). *Top400. A top-down crime prevention strategy in Amsterdam*. Public Interest Litigation Project.
Jansen, J., T. van Valkengoed, S. Veenstra & W.P. Stol (2020). *Level-Up! Kennis voor politiewerk in een digitale samenleving*. NHL Stenden Hogeschool/Politieacademie.
Jansen, J., S. Westers, W. Scheurs, M. Berkenpas, G. Alpár & W. Stol (2023). *De rol van encryptie in de opsporing. Belemmeringen en mogelijkheden*. NHL Stenden Hogeschool.
Joh, E.E. (2016). 'The new surveillance discretion: automated suspicion, big data, and policing'. *Harvard Law & Policy Review*, 15, p. 15-42.

Joh, E.E. (2017). 'Feeding the machine: policing, crime data & algorithms'. *William & Mary Bill of Rights Journal*, 26(2), p. 287-302.
Joh, E.E. (2018a). 'Artificial intelligence and policing: first questions'. *Seattle University Law Review*, 41, p. 1139-1144.
Joh, E.E. (2018b). 'Artificial intelligence and policing: hints in the Carpenter decision'. *Ohio Stare Journal of Criminal Law*, 16, p. 281-290.
Joh, E.E. (2019). 'Policing the smart city'. *International Journal of Law in Context*, 15, p. 177-182.
Joh, E.E. (2020). 'Increasing automation in policing'. *Communications of the ACM*, 63(1), p. 20-22.
Jones, B. (2020). *Data literacy fundamentals. Understanding the power & value of data*. Data Literacy Press.
Jong, J. de (2018). *Het mysterie van de verdwenen criminaliteit*. Centraal Bureau voor de Statistiek.

Kassab, H. & J. Rosen (2019). 'General trends in drug and organized crime on a global scale'. In: H. Kassab & J. Rosen (Eds.), Illicit markets, organized crime, and global security (p. 87-109). Palgrave Macmillan.
Kearns, I. & R. Muir (2019). *Data driven policing and public value*. The Police Foundation.
Keijser, B., G. Veldhuis & S. Huisman (2020). 'Nieuwe analysemethode ondermijning'. *Het Tijdschrift voor de Politie*, 82(1), p. 40-45.
Kelleher, J.D. & B. Tierney (2018). *Data science*. The MIT Press.
Khalfa, R. & W. Hardyns (2023). '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* (p. 179-206). Gompel & Svacina.
Kirby, S. & S. Keay (2021). *Improving intelligence analysis in policing*. Routledge.
Kirby, S. & N. Snow (2016). 'Praxis and the disruption of organized crime groups'. *Trends in Organized Crime*, 19(2), p. 111-124.
Kitchin, R. (2014). *The data revolution. Big data, open data, data infrastructures and their consequences*. Sage Publications.
Klerks, P. (2020). *Door leugens verleid. Hoe je fake news en andere vormen van manipulatie herkent en bestrijdt*. Prometheus.
Klerks, P. & K. Vink-Teeven (2020). 'De inzet van data-analysetechnologie ter bevordering van de informatiegestuurde opsporing'. In: J. Janssens, W. Broer, M. Crispel & R. Salet (Eds.), *Informatiegestuurde politie* (p. 163-176). Gompel & Svacina.
Knaap, G. van der (2022). *Van Aristoteles tot algoritme. Filosofie van kunstmatige intelligentie*. Boom uitgevers.
Knoke, D. (2015). 'Emerging trends in social network analysis of terrorism and counterterrorism'. In: R.A. Scott, S.M. Kosslyn & S. M. Buchmann (Eds.), *Emerging trends in the social and behavioral sciences*. John Wiley & Sons.

Kock, P.A.M.G. de (2014). *Anticipating criminal behaviour: using the narrative in crime-related data*. Wolf Legal Publishers.
Koelewijn, W.I. (2009). *Privacy en politiegegevens. Over geautomatiseerde normatieve informatie-uitwisseling*. Universiteit Leiden.
Koning, B. de (2017). 'Opheldering verzocht? Over de drastische daling van het aantal opgehelderde misdrijven'. *Justitiële Verkenningen*, 43(4), p. 37-46.
Kool, D. de, B. Vermeeren & B. Steijn (2020). *Kunstmatige intelligentie bij de politie: praktische en sociale lessen ten aanzien van het aangifteproces*. Rotterdam: Erasmus University.
Kool, D. de, B. Vermeeren & B. Steijn (2023). *Kunstmatige intelligentie bij de politie. Een internationale literatuurstudie*. Politie & Wetenschap.
Kool, L., J. Timmer, L. Royakkers & R. van Est (2017). *Opwaarderen. Borgen van publieke waarden in de digitale samenleving*. Rathenau Instituut.
Koolstra, S., B. de Veer & T. Veltman (2021). *Dit is kunstmatige intelligentie. Een introductie in de technologie die ons leven steeds meer bepaalt*. Van Haren Publishing.
Koops, B-J. (2013). 'Police investigations in internet open sources: procedural-law issues'. *Computer Law & Security Review*, 29, p. 654-665.
Kop, N. (2012). *Van opsporing naar criminaliteitsbeheersing. Vijf strategische implicaties*. Politieacademie.
Kop, N. & P. Klerks (2008). *Doctrine intelligencegestuurd politiewerk*. Politieacademie.
Koper, C.S. & C. Lum (2019). 'Technology in policing: critic. The limits of police technology'. In: D. Weisburd & A.A. Braga (eds.), *Police innovation. Contrasting perspectives* (p. 517-543). Cambridge University Press.
Koper, C.S., C. Lum & J.J. Willis (2014). '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*, *8*(2), p. 212-221.
Koppen, P. van (2022). *De som van alle bewijs: scenario's in strafzaken*. Uitgeverij de Kring.
Kort, J. & R. Spithoven (2021). *De coronacrisis als cyberkeerpunt? Op zoek naar lokaal handelingsperspectief in de aanpak van gedigitaliseerde criminaliteit*. Politie Nederland/ Hogeschool Saxion.
Kotzé, J. (2019). *The myth of the 'crime decline'. Exploring change and continuity in crime and harm*. Routledge.
Kouwenhoven, R.M. & , L. Kleijer-Kool (2016). *Die pakken we toch niet op? Afstemming tussen politie en Openbaar Ministerie in zaken van veelvoorkomende criminaliteit*. Reed Business.
Kraus, S., P. Jones, N. Kailer, A. Weinmann, N. Chaparro-Banegas & N. Roig-Tierno (2021). 'Digital transformation: an overview of the current state of the art of research'. SAGE Open, 11(3).
Krikken, E. (2021). *Op waarden geschat. Living lab digitale perimeter*. Bits of Freedom.
Kroes, P., H. ter Veen & N. Kop (2023). *Bekrachtigen van innovatie. Opschalen in de politiepraktijk*. Politieacademie.

Kruisbergen, E.W., E.R. Leukfeldt, E.R. Kleemans & R.A. Roks (2018). *Georganiseerde criminaliteit en ICT. Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit*. Wetenschappelijk Onderzoek- en Documentatiecentrum.
Kruisbergen, E.W., R.A. Roks & E.R. Kleemans (2019). *Georganiseerde criminaliteit in Nederland: daders, verwevenheid en opsporing*. Wetenschappelijk Onderzoek- en Documentatiecentrum.
Kulk, S. & S. van Deursen (2020). *Juridische aspecten van algoritmen die besluiten nemen. Een verkennend onderzoek*. Wetenschappelijk Onderzoek- en Documentatiecentrum.
Kuppens, J., E. Bervoets & H. Ferwerda (2010). *Poortwachters van de politie. Meldkamers in dagelijks perspectief*. Reed Business.

Landman, W. (2015). *Blauwe patronen. Betekenisgeving in politiewerk*. Boom Lemma.
Landman, W. (2022). 'Tussen politiemens en politiemachine. Discretionaire ruimte in het tijdperk van datagedreven politiewerk'. In: A. Verhage, R. Salet, F. Schuermans & J. Nap (Eds.), *Discretionaire ruimte in de handhaving* (p. 81-99). Gompel & Svacina.
Landman, W. (2023). 'Spanningen bij politiewerk op het web. Online gegevensgaring in een woelige samenleving'. *Het Tijdschrift voor de Politie*, *85*(2), p. 10-14.
Landman, W. & S. Groothuis (2022). *Politiewerk op het web. Een verkennend onderzoek naar online gegevensvergaring*. Sdu Uitgevers.
Landman, W. & L. Kleijer-Kool (2016). *Boeven vangen. Een onderzoek naar proactief politieoptreden*. Reed Business.
Landman, W., R.M. Kouwenhoven & M. Brussen (2020). *Kijk naar het systeem. Begrijpen en beïnvloeden van opsporingspraktijken*. Sdu Uitgevers.
Lane, J. (2019). *The digital street*. Oxford University Press.
Lanting, M. (2021). *Uit het transformatiemoeras. De 5 faalfactoren bij de digitalisering van organisaties*. Uitgeverij Business Contact.
Lauwaert, L. (2021). *Wij, robots. Een filosofische blik op technologie en artificiële intelligentie*. Uitgeverij LannooCampus.
Lavorgna, A. (2019). 'Analysis and prevention of organized crime'. In: R. Wortley, A. Sidebottom, N. Tilley & G. Laycock (Eds.), *Routledge handbook of crime science* (p. 223-232). Routledge.
Leiden, I. van & H. Ferwerda (2006). *Cold cases, een hot issue. Toepassing en opbrengsten van hernieuwd onderzoek naar onopgeloste kapitale delicten*. Reed Business.
Leistra, G. (2020). *De drugsmaffia dicteert. De moord op Derk Wiersum en de ondermijning van onze rechtsstaat*. De Geus.
Leito, T.L.M., S.R. van Bemmel & F. Noteboom (2021). *Het misdrijf voorbij. Een verkenning naar criminele uitbuiting in Rotterdam*. Centrum tegen Kinderhandel en Mensenhandel.
Leonardi, P.& T. Neeley (2022). *The digital mindset. What it really takes to thrive in the age of data, algorithms and AI*. Harvard Business Review Press.
Leukfeldt, R. (2018). *De 'human factor' in cybersecurity: Intreerede*. Haagse Hogeschool.

Leukfeldt, E.R. & T.J. Holt (2022). 'Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals'. *Computers in Human Behavior*, 126, p. 1-9.
Leukfeldt, E.R., E.R. Kleemans & W.P. Stol (2017). 'Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks'. *British Journal of Criminology*, 57(3), p. 704-722.
Leukfeldt, R., R. Notté & M. Malsch (2018). *Slachtofferschap van online criminaliteit. Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit*. Nederlands Studiecentrum Criminaliteit en Rechtshandhaving.
Leukfeldt, E.R. & R.A. Roks (2021). 'Cybercrimes on the streets of the Netherlands? An exploration of the intersection of cybercrimes and street crimes'. *Deviant behavior*, 42(11), p. 1-12.
Levine, E.S., J. Tisch, A. Tasso & M. Joy (2017). 'The New York City police department's domain awareness system'. *Interfaces*, *47*(1), 70-84.
Liempt, P. van (2022). *Misdaad en straf in de polder. Het OM aan het woord*. Prometheus.
Lin, P.K. (2022). *Machine see, machine do. How technology mirrors bias in our criminal justice system*. New Degree Press.
Linder, T. (2019). 'Surveillance capitalism and platform policing: the surveillant assemblage-as-a-service'. *Surveillance & Society*, 17(1/2), p. 76-82.
Lipsky, M. (2010). *Street-level bureaucracy. Dilemmas of the individual in public services (30th anniversary expanded edition)*. Russel Sage Foundation.
Lodder, A.R., N.S. van der Meulen, T.H.A. Wisman, L. Meij & C.M.M. Zwinkels (2014*). Big data, big consequences? Een verkenning naar privacy en big data gebruik binnen de opsporing, vervolg en rechtspraak*. Vrije Universiteit Amsterdam.
Lomell, H.M. (2018). 'Investigation or instigation? Enforcing grooming legislation'. In: N.R. Fyfe, H.O.I. Gundhus & K.V. Rønn (Eds.). *Moral issues in intelligence-led policing* (p. 43-61). Routledge.
Loo, H. van der & P. Davidson (2022). *Teaming. De nieuwe realiteit van samenwerken*. VMN Media.
Lum, C., C.S. Koper & J. Willis (2017). 'Understanding the limits of technology's impact on police effectiveness'. *Police Quarterly*, 20(2), p. 135-136.
Luyendijk, J. (2017). *Kunnen we praten*. Uitgeverij Atlas Contact.
Lyon, D. (2018). *Culture of surveillance. Watching as a way of life*. Polity Press.

Madiega, T., P. Car & M. Niestadt (2022). *Metaverse: opportunities, risks and policy implications*. European Parliamentary Research Service.
Madiega, T. (2023). *Artificial intelligence act*. European Parliamentary Research Service.
Maggiori, E. (2023). *Smart until its'dumb. Why artificial intelligence keeps making epic mistakes (and why the AI bubble will burst)*. Applied Maths Ltd.

Mali, B., C. Bronkorst-Giesen & M. den Hengst (2017). *Predictive policing: lessen voor de toekomst. Een evaluatie van de landelijke pilot*. Politieacademie.
Mandour, Y., D. van der Heijden & S. Turnhout (2020). *De strategie van de kreeft. Bouw aan echte vernieuwing*. Van Duuren Management.
Mannens, E. (2021). 'Wat je moet weten over AI'. In: J. de Bruyne & N. Bouteca (Red.), *Artificiële intelligentie en maatschappij* (pp. 17-48). Gompel&Svacina.
Manning, P.K. (1980). *The Narcs' game. Organizational and informational limits on drug law enforcement*. The MIT Press.
Manning, P.K. (2008). *The technology of policing. Crime mapping, information technology, and the rationality of crime control*. New York University Press.
Manning, P.K. (2010). *Democratic policing in a changing world*. Paradigm Publishers.
Mapes, A.A. (2017). *Rapid DNA technologies at the crime scene. 'CSI' fiction matching reality*. University of Amsterdam.
Marciniak, D. (2021). *Data-driven policing. How digital technologies transform the practice and governance of policing*. University of Essex.
Marx, G.T. (2007). 'The engineering of social control: policing and technology'. *Policing: A Journal of Policy and Practice*, 1(1), p. 46-56.
Marx, G.T. (2016). *Windows into the soul. Surveillance and society in an age of high technology*. The University of Chicago Press.
McCulloch, J. & D. Wilson (2015). *Pre-crime. Pre-emption, precaution and the future*. Routledge.
McDaniel, J.L.M. & K.G. Pease (2021a). 'Introduction'. In: J.L.M. McDaniel & K.G. Pease (Eds). *Predictive policing and artificial intelligence* (p. 1-38). Routledge.
McDaniel, J.L.M. & K.G. Pease (2021b). 'Policing, AI and choice architecture'. In: J.L.M. McDaniel & K.G. Pease (Eds), *Predictive policing and artificial intelligence* (p. 79-110). Routledge.
McDermott, J., J. Bargent, D. den Held & M.F. Ramírez (2021). *The cocaine pipeline to Europe*. Global Initiative Against Transnational Organized Crime.
McFadzien, K., A. Pughsley, A.M. Featherstone & J.M. Phillips (2020). 'The Evidence-Based Investigative Tool (EBIT): a legitimacy-conscious statistical triage process for high-volume crimes'. *Cambridge Journal of Evidence-Based Policing*, 4, p. 218-232.
McGuire, M.R. (2017). 'Technology, crime and technology control: contexts and history'. In: M.R. McGuire & T.J. Holt (Eds.), *The Routledge handbook of technology, crime and justice* (p. 35-60). Routledge.
McGuire, M.R. (2021). 'The laughing policebot: automation and the end of policing', *Policing and Society*, 31(1), 20-36.
McKinsey & Company (2022). *Value creation in the metaverse. The real business of the virtual world*. New York.
Meconi, T. & H. Henseler (2022). 'Digitale sporen in smartphones. Een kennismaking met pattern-of-life forensics'. *Expertise en Recht*, 3, p. 70-77.
Meershoek, G. (2007). *De geschiedenis van de Nederlandse politie. De gemeentepolitie in een veranderende samenleving*. Boom.

Meershoek, G. (2018). 'Bestuurlijke focus en sociale weerbaarheid bij de georganiseerde- misdaadbestrijding'. *Het Tijdschrift voor de Politie,* 80(1), p. 6-10.
Meeteren, M. van (2022). 'Complotdenken in tijden van online desinformatie'. *Boom strafblad*, 5, p. 211-217.
Mehlbaum, S., K. van den Akker, A. Verweij & A. Wester (2021). *Zuiver op de graat? Over de betrokkenheid van de visserij bij maritieme drugssmokkel*. Sdu Uitgevers.
Mehlbaum, S., I. van Duijneveldt, R. Holvast & D. van Arkel (2014). 'Organiseren voor heterdaadkracht'. *Het Tijdschrift voor de Politie*, 76(1), p. 6-11.
Meijer, A. & M. Wessels (2019). 'Predictive policing: review of benefits and drawbacks'. *International Journal of Public Administration*, 42(12), p. 1031-1039.
Meijer, A., L. Lorenz & M. Wessels (2021). 'Algorithmization of bureaucratic organizations: using a practice lens to study how context shapes predictive policing systems'. *Public Administration Review*, 81(5), p. 837-846.
Meulenbroek, L. (2021). *DNA zoekmachine. Databanken en hun slagkracht bij opsporing en identificatie*. Bertram + de Leeuw Uitgevers.
Milivojevic, S. (2021). *Crime and punishment in the future internet. Digital frontier technologies and criminology in the twenty-first century*. Routledge.
Miller, B.H. (2018). 'Open Source Intelligence (OSINT): an oxymoron?'. *International Journal of Intelligence and CounterIntelligence*, 31(4), p. 702-719.
Miltenburg, E., B. Geurkink, S. Tunderman, D. Beekers & J. den Ridder (2022). *Burgerperspectieven 2022. Bericht 2*. Sociaal en Cultureel Planbureau.
Mishra, P. (2017). *Age of anger. A history of the present*. Allen Lane.
Modderkolk, H. (2019). *Het is oorlog maar niemand die het ziet*. Uitgeverij Podium.
Molder, R.M. te (2022). 'Digitaal forensische zoekmachines, effectieve verdedigingsrechten en de modernisering van het Wetboek van Strafvordering: is aanpassing van het conceptwetsvoorstel gewenst?'. *Boom Strafblad*, 5, p. 178-186.
Molder, R.M. te, M.J. Dubelaar, M.I. Fedorova, S.M.A. Lestrade & T.F. Walree (2023). 'Naar een duidelijker juridisch kader voor geautomatiseerde data-analyse in de opsporing'. *Computerrecht*, 64(2), p. 110-117.
Mols, B. (2023). *Slim, slimmer, slimst. Hoe kunstmatige intelligentie de mens een turboboost geeft*. New Scientist Pocket Science.
Morozov, E. (2013). *To save everything, click here. The folly of technological solutionism*. Public Affairs.
Moyle, L., A. Childs, R. Coomber & M.J. Barratt (2019). '#Drugsforsale: an exploration of the use of social media and encrypted messaging apps to supply and access drugs'. *International Journal of Drug Policy*, 63, p. 101-110.
Mulder, H. & H. Schönfeld (2023). Historie als basis voor de toekomst. Een beschouwing over IT en de politieorganisatie. In: J. van Hoorn & M. van Bavel (Red.), *Onze politie in een kwetsbare rechtstaat* (p. 127-159). Gompel&Svacina.
Müller, J-W. (2021). *Wat is echte democratie?* Nieuw Amsterdam.
Mutsaers, P. & T. van Nuenen (2023). 'Predictively policed: the Dutch CAS case and its forerunners'. In: J. Beek, T. Bierschenk, A. Kolloch & B. Meyer (Eds.), *Policing race, ethnicity and culture* (p. 72-94). Manchester University Press.

Nap, J.A. (2012). *Vragen naar goed politiewerk: belang-stellend ontwikkelen van de alledaagse praktijk. Een proeve van normatieve professionalisering*. Boom Lemma Uitgevers.
Nap, J.A. (2014). *Macht ten goede?! Sterke arm in een complexe samenleving*. Politieacademie.
Nationaal Coördinator Terrorismebestrijding en Veiligheid (2022a). *Cybersecuritybeeld Nederland 2022*. NCTV.
Nationaal Coördinator Terrorismebestrijding en Veiligheid (2022b). *Dreigingsbeeld terrorisme Nederland 57*. NCTV.
Nationaal Coördinator Terrorismebestrijding en Veiligheid (2023). *Cybersecuritybeeld Nederland 2023*. NCTV.
Nelen, H., K. van Wingerde, L. Bisschop & R. Moerland (2023). *Koers bepalen. Over de lessen van de versterking aanpak georganiseerde drugscriminaliteit*. Boom Criminologie.
Newburn, T. & S. Hayman (2002). *Policing, surveillance and social control. CCTV and police monitoring of suspects*. Willan Publishing.
Niculescu-Dincă, V. (2016). *Policing matter(s). Towards a sedimentology of suspicion in technologically mediated surveillance*. Universitaire pers Maastricht.
Noordanus, P.G.A. (2020*). Een pact voor de rechtsstaat. Een sterke terugdringing van drugscriminaliteit in tien jaar*. Aanjaagteam Ondermijning.
Novitzky, P., B. Kokkeler & P. Verbeek (2018). 'The dual-use of drones'. *Tijdschrift voor veiligheid,* 17(1-2), p. 79-95.

O'Neil, C. (2016). *Weapons of math destruction. How big data increases inequality and threatens democracy*. Broadway Books.
Odekerken, D. & F. Bex (2020). 'Towards transparent human-in-the-loop classification of fraudulent web shops'. *Legal Knowledge and Information Systems*, p. 239-242.
Odinet, G., M.A. Verhoeven, R.L.D. Pool & C.J. de Poot (2017). *Organised cybercrime in the Netherlands. Empirical findings and implications for law enforcement*. Wetenschappelijk Onderzoek- en Documentatiecentrum.
Oerlemans, J.J. (2017a). *Investigating cybercrime*. Amsterdam University Press.
Oerlemans, J.J. (2017b). *Normering van digitale opsporingsmethoden*. Nederlandse Defensie Academie.
Oerlemans, J.J. (2020a). *Grenzen stellen aan datahonger. De bescherming van de nationale veiligheid in een democratische rechtsstaat*. Universiteit Utrecht.
Oerlemans, J.J. (2020b). 'Cybercriminaliteit en opsporing'. In: W. van der Wagen, J.J. Oerlemans & M. Weulen Kranenbarg (Red.), *Basisboek cybercriminaliteit. Een criminologisch overzicht voor studie en praktijk* (p. 195-258). Boom Criminologie.
Oerlemans, J.J. & W. van der Wagen (2020). 'Verschijningsvormen van cybercriminaliteit'. In: W. van der Wagen, J.J. Oerlemans & M. Weulen Kranenbarg (Red.), *Basisboek cybercriminaliteit. Een criminologisch overzicht voor studie en praktijk* (p. 55-97). Boom criminologie.
Oerlemans, J.J. & R. van Wegberg (2019). 'Opsporing en bestrijding van online drugsmarkten'. *Strafblad* (5), p. 25-31.

Oosterloo, S. & G. Van Schie (2018). 'The politics and biases of the 'Crime Anticipation System' of the Dutch Police'. *Proceedings of International Workshop on Bias in Information, Algorithms, and Systems*, 2103, p. 30-41.
Openbaar Ministerie & Politie (2020). *Kwaliteitskader big data*. OM/Politie Nederland.
Os, P. van, G. van den Brink & J. Baardewijk (2007). *Heterdaadkracht. Aanhoudend in de buurt*. Politieacademie.
Osinga, F., W.J. Derksen, T. de Bel, D. Broeders, P. Ducheine, M. Janssen, S. Klous & R. Prins (2022). *Digitalisering en liberale kernwaarden. Vrijheid door grenzen te stellen in de digitale wereld*. Gompel & Svacina.

Pasquale, F. (2016). *The black box society. The secret algorithms that control money and information*. Harvard Business Review Press.
Pasquale, F. (2020). *The new law of robotics. Defending human expertise in the age of AI*. The Belknap Press.
Passchier, R. (2021). *Artificiële intelligentie en de rechtsstaat. Over verschuivende overheidsmacht, Big Tech en de noodzaak van constitutioneel onderhoud*. Boom Juridisch.
Paulissen, W. (2022). 'De aanpak van ondermijnende criminaliteit en drugs'. *Het Tijdschrift voor de Politie*, 84(2), p. 6-8.
Pauw, E. de (2019). 'Technologie in beweging'. In: E. Devroe, A. Schmidt, L. Gunther Moor & P. Ponsaers (Eds.), *De essentie van politiewerk* (p. 81-90). Gompel & Svacina.
Pearl, J. & D. Mackenzie (2019). *Het boek waarom. De nieuwe wetenschap van oorzaak en gevolg*. Maven Publishing.
Peeters, R. & M.B. Schuilenburg (2021). 'The algorithmic society. An introduction'. In: M. Schuilenburg & R. Peeters (Eds.), *The algorithmic society. Technology, power and knowledge* (p. 15-40). Routledge.
Peeters, T. & T. van Dongen (2022*). Schijnwerpers op de straat. Over de lessen van de aanpak van de Van Wougroep en andere criminele jeugdgroepen*. Verwey-Jonker Instituut.
Peters, L.J.J. (2018). *Dealen met ondermijningsdelicten. Naar een efficiënte strafprocedure voor ondermijnende criminaliteit*. Wolters Kluwer.
Plas, A. van der & C. Brown (2017). 'Inwinning'. In; M. den Hengst, T. ten Brink & J. ter Mors (Red.), *Informatiegestuurd politiewerk in de praktijk* (p. 179-192). Vakmedianet.
Plas, T. van der, G. Kuijlaars & H. Geveke (2022). 'Nederlandse politie en ketenpartners onderzoeken noodzakelijke ontwikkelsprongen voor versnelling in digitale transformatie'. In: A. van Dijk, P. de Baets, L. Gunther Moor, E. Devroe & S. Zouridis (Eds.), *Politie en rechtsstaat in de gedigitaliseerde samenleving* (p. 63-82). Gompel & Svacina.
Politie (2017). *Plan van aanpak operationele proeftuin sensing Roermond*. Politie Nederland.
Politie (2018). *Privacy & security by design. Uitvoeringskader voor de omgang met gegevens*. Politie Nederland.
Politie (2019). *Begeleidingsethiek bij de politie. Verslag van de eerste ethiektafels*. Politie Nederland.
Politie (2022). *Begroting en beheerplan 2023-2026*. Politie Nederland.

Politie (2023). *Inzetkader Gezichtsherkenningstechnologie Politie. Een eerste kader ter toetsing van operationele inzetten*. Politie Nederland.
Poot, C.J. de (2017). *De reconstructie van strafbare feiten*. Vrije Universiteit Amsterdam.
Poot, C.J. de (2021). 'Het gebruik van DNA in het opsporingsproces'. *Justitiële Verkenningen*, 47(1), p. 20-43.
Poot, C.J. de, R.J. Bokhorst, P.J. Koppen & E.R. Muller (2004). *Rechercheportret. Over dilemma's in de opsporing*. Kluwer.
PricewaterhouseCoopers (2021). *Onderzoek personele en materiële lasten 2021-2025*. PWC.
Prins, V.A. (2020). *Sensoren, risicoscores en mensenrechten. Een onderzoek naar de mensenrechtenimplicaties van het predictive policingproject Sensing Mobiel Banditisme in Roermond*. Universiteit Utrecht.
Punch, M. (1983). *De Warmoesstraat. Politiewerk in de binnenstad. Een etnografische studie van politiewerk in Amsterdam*. Van Loghum Slaterus.

Quick, D. & K. Raymond Choo (2016). 'Big forensic data reduction: digital forensic images and electronic evidence'. *Cluster Computing*, 19, p. 723-740.

Raad voor het Openbaar Bestuur (2021). *Sturen of gestuurd worden? Over de legitimiteit van het sturen met data*. ROB.
Rasch, M. (2020). *Frictie. Ethiek in tijden van dataïsme*. De Bezige Bij.
Rashedi, J. (2022). *The data-driven organization. Using data for the success of your company*. Springer.
Ratcliffe, J.H. (2016). *Intelligence-led policing*. Routledge.
Ratcliffe, J.H. (2019). 'Advocate: predictive policing'. In: D. Weisburd & A.A. Braga (Eds.), *Police innovation. Contrasting perspectives* (p. 347-365). Cambridge University Press.
Ratcliffe, J.H., R.B. Taylor, A.P. Askey, K. Thomas, J. Grasso, K.J. Bethel, R. Fisher & J. Koehnlei (2021). 'The Philadelphia predictive policing experiment'. *Journal of Experimental Criminology*, 17, p. 15-41.
Ratcliffe, J.H., R.B. Taylor & R. Fisher (2020). 'Conflicts and congruencies between predictive policing and the patrol officer's craft'. *Policing and Society*, 30(6), p. 639-655.
Rathenau Instituut (2021b). *De prijs van een surveillancesamenleving. Een overzichtsessay over betekenis, werking en risico's van surveillerende computers*. Rathenau Instituut.
Rathenau Instituut (2023). *Moeilijke keuzes en meer informatievoorziening. Bericht aan het parlement*. Rathenau Instituut.
Rauch, J. (2021). *The constitution of knowledge. A defense of truth*. Brookings Institution Press.
Reenen, P. van (2010). 'De tanden van de politie'. In; B. van Stokkom, J. Terpstra & L. Gunther Moor (Red.), *De politie en haar opdracht. De kerntakendiscussie voorbij* (p. 117-137). Maklu Uitgevers.

Reenen, P. van (2012). *Tot op heden is dergelijk onderzoek niet verricht. De effectiviteit van de politie en haar legitimiteit: studies tegen het licht gehouden*. Reed Business.
Reijneveld, R. (2017). 'Analyse'. In: M. den Hengst, T. ten Brink & J. ter Mors (Red.), *Informatiegestuurd politiewerk in de praktijk* (p. 133-145). Vakmedianet.
Rest, J.H.C. van, T. Attema, T. Timan, R.J.M. den Hollander & G.P. van Voorthuijsen (2021). *Privacy bescherming bij niet-coöperatieve gezichtsherkenning*. TNO.
Rienks, R. (2015). *Predictive policing. Kansen voor een veiligere toekomst*. Politieacademie.
Rienks, R. & M.B. Schuilenburg (2020). 'Wat is er nieuw aan het voorspellen van criminaliteit? Over de ambities en knelpinten bij de implementatie van predictive policing'. In: J. Janssens, W. Broer, M. Crispel & R. Salet (Eds.). *Informatiegestuurde politie* (p. 39-54). Gompel & Svacina.
Robison, D. & C. Scogings (2018). 'The detection of criminal groups in real-world fused data: using the graph-mining algorithm "GraphExtract"'. *Security Informatics*, 7(2). https://doi.org/10.1186/s13388-018-0031-9.
Roest, D. (2021). 'TROI: een denksprong naar radicale flexibiliteit'. *Het Tijdschrift voor de Politie*, 83(3), p. 15-17.
Roest, D. (2023). '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* (p. 91-106). Gompel & Svacina.
Rogers, M. (2017). 'Technology and digital forensics'. In: M.R. McGuire & T.J. Holt (Eds.), *The Routledge handbook of technology, crime and justice* (p. 406-415). Routledge.
Roks, R.A. & J. Hendriksen (2021). '"Laat je niet misleiden door afwijkende prijzen". Een exploratieve studie naar de ambiguïteit van betrouwbaarheid van cocaïnedealers op Telegram Messenger'. *Tijdschrift voor Criminologie*, *63*(2), p. 212-235.
Roks, R.A. & N. Monshouwer (2020). 'F-gamers die "mapsen", "swipen" en "bonken": een netnografisch onderzoek naar fraude en oplichting op Telegram Messenger'. *Justitiële Verkenningen*, 46(2), p. 44-58.
Roks, R.A., E.R. Leukfeldt & J.A. Densley (2020). 'The hybridization of street offending in the Netherlands'. *The British Journal of Criminology*, 61(4), p. 926-945.
Römkes, R. & J. van Poppel (2007). *Bruikbaarheid van het risicotaxatie-instrument huiselijk geweld. Een eerste evaluatie*. IVA.
Roo, R.H.D. de & C.J. de Poot (2022). *LocalDNA. De ontwikkeling en werking van een snelle DNA onderzoeksroute in de opsporingspraktijk. Wetenschappelijke rapportage*. Hogeschool van Amsterdam/Politieacademie.
Roolvink, S., S. Kuijvenhoven & M. Huijstee (2022). 'Wat is de rol van de politie bij metaverse?'. *Het Tijdschrift voor de Politie*, 84(3), p. 36-39.
Rosenthal, U. (2007). 'Politie en staat'. In: C.J.C. Fijnaut, E.R. Muller, U. Rosenthal & E.J. van der Torre (Red.). *Politie. Studies over haar werking en organisatie* (p.19-43). Kluwer.
Rossy, Q. & C. Morselli (2018). 'The contribution of forensic science to the analysis of criminal networks'. In: Q. Rossy, D. Décary-Hétu, O. Delémont & M. Mulone (Eds.),

The Routledge international handbook of forensic intelligence and criminology (p. 191-204). Routledge.
Roubini, N. (2022). *Megathreats. The ten trends that imperil our future, and how to survive them*. John Murray.
Rovers, B. & M. Jans (2014). *Risicotaxatie-instrument geweldplegers (RTI-Geweld). Verantwoordingsdocument*. Bureau voor Toegepast Veiligheidsonderzoek.
Rovers, B., H. Moors, M. Jacobs & M. Jans (2012). *Toolbox persoonsgerichte aanpak high impact crimes*. Ministerie van Veiligheid en Justitie.

Sadin, E. (2021). *Het tijdperk van de ik-tiran. Het einde van de gemeenschappelijke wereld*. Wereldbibliotheek.
Sanders, C.B. & J. Chan (2021). 'The challenges facing Canadian police in making use of big data analytics'. In: D. Lyon & D.M. Wood (Eds.), *Big data surveillance and security intelligence. The Canadian case* (p. 180-194). UBC Press.
Sandt, E. van de, M. den Hengst, P. de Bruine, R. Westerhof & S. van der Maden (2022). '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). Gompel & Svacina.
Santvoord, V.D. van & T. van Ruitenburg (2022*).* 'Financial crime scripting: introducing a financial perspective to the Dutch cocaine trade'. *The Police Journal,* 0(0). https://doi.org/10.1177/0032258X221083449.
Sartor, G. & A. Loreggia (2022). *The impact of Pegasus on fundamental rights and democratic processes.* European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs.
Scassa, T. (2017). 'Law enforcement in the age of big data and surveillance intermediaries: transparency challenges'. *SCRIPTed*, 14(2), p. 239-284.
Schaik, A. van (2022). 'Hoe blauw is de recherche? Een onderzoek naar de drie recherche-identiteiten'. In: J. Janssen, B. Defrancq, D. Schaap & P. Ponsaers (Eds.), *Politiecultuur* (p. 17-40). Gompel & Svacina.
Schendel, S. van & C. Cuijpers (2023). 'Big-datatoepassingen in de opsporing; een pleidooi voor de integratie van fundamentele mensenrechtenbescherming in het strafprocesrecht'. In: T. Snaphaan, W. Hardyns, A. van Dijk, R. Spithoven & R. van Brakel (Eds.), *Big data policing* (p. 135-150). Gompel & Svacina.
Schermer, B.W. (2022). *De gespannen relatie tussen privacy en cybercrime*. Universiteit Leiden.
Schermer, B.W. & J. van Ham (2021). *Regulering van immersieve technologieën*. Wetenschappelijk Onderzoek- en Documentatiecentrum.
Schermer, B.W. & J.J. Oerlemans (2022). 'De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie?'. *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 2, p. 82-89.

Schermer, B.W. & M. Galič (2023). 'De bescherming van algoritmische groepen bij profilering en datagedreven politiewerk. Van individuele naar group privacy?' *Boom Strafblad*, 2, p. 56-65.
Scherpenisse, J., M.J.W. van Twist & J. Schram (2017). *Ondertussen in de Spaanse polder. Experimenteren met een nieuwe aanpak van ondermijnende criminaliteit*. Nederlandse School voor het Openbaar Bestuur.
Schick, N. (2020). *Deep fakes and the infocalypse. What you urgently need to know*. Octopus Publishing Group.
Schiff, D.S., K.J. Schiff & P. Pierson (2021). 'Assessing public value failure in government adoption of artificial intelligence'. *Public Administration*, 100(3), p. 653-673.
Schiks, J., S. van 't Hoff-de Goede & R. Leukfeldt (2022). *Op zoek naar de parels bij de regionale en lokale aanpak van cybercriminaliteit en gedigitaliseerde criminaliteit. Een verkennend onderzoek*. Politie & Wetenschap.
Schnitlzer, H. (2021). *Wij nihilisten. Een zoektocht naar de geest van digitalisering.* De Bezige Bij.
Scholtens, A., M. de Hengst & R. Waterreus (2016). *Het real-time informeren van noodhulpeenheden. Een onderzoek naar de RTI-functie om frontlijnpolitiefunctionarissen snel te voorzien van relevante informatie*. Reed Business.
Schrama, V., J. van de Laarschot, C. Volten & R. van Wegberg (2022). *Virtuele valuta. Handelingsperspectieven voor data-gedreven opsporing*. TU Delft.
Schuilenburg, M.B. (2016). 'Predictive policing. De opkomst van een gedachtenpolitie?', *Ars aequi*, 65(12), p. 931-936.
Schuilenburg, M.B. (2023). '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* (p. 53-70). Gompel & Svacina.
Schuilenburg, M.B. & M. Soudijn (2021). 'Big data in het veiligheidsdomein: Onderzoek naar big data-toepassingen bij de politie en de positieve effecten hiervan voor de politieorganisatie.' *Tijdschrift voor Veiligheid*, 21(4): p. 1-19.
Schuilenburg, M.B. & M. Wessels (2022). 'Een afwegingskader bij het invoeren van nieuwe technologie. Vier handvatten voor betrouwbare algoritmische toepassingen in het politiewerk'. *Het Tijdschrift voor de Politie*, 84(3), p. 11-15.
Schwab, K. (2017). *The fourth industrial revolution*. Penguin Random House.
Seymoens, T., L. van Audenhoeve, F. Heymans, M. Brengman, P. Duysburgh, I. Marien & A. Jacobs (2020).'Datageletterdheid als voorwaarde voor een succesvolle AI-transformatie'. In: J. de Bruyne & N. Bouteca (Red.), *Artificiële intelligentie en maatschappij* (pp. 75-96). Gompel&Svacina.
Shapiro, A. (2017). 'Reform predictive policing'. *Nature*, 541, p. 458-460.
Shapiro, A. (2020). *Design, control, predict. Logistical governance in the smart city*. University of Minnesota Press.
Shneiderman, B. (2022). *Human-centered AI*. Oxford University Press.

Shon, P.C. & C.D. O'Connor (2021). 'Why policing the risk society became a footnote in American police studies: A missed opportunity to move police theorizing forward'. *The Police Journal*, 94(2), p. 222-238.
Silfversten, E., M. Favaro, L. Slapakova, S. Ishikawa, J. Liu & A. Salas (2020). *Exploring the use of Zcash cryptocurrency for illicit or criminal purposes*. RAND Corporation.
Simmons, R. (2019). *Smart surveillance. How to interpret the fourth amendment in the twenty-first century*. Cambridge University Press.
Skogan, W.G. (2019). 'The future of CCTV'. *Criminology & Public Policy*, 18(1), p. 161-166.
Sloot, B. van der, Y. Wagensveld & B-J. Koops (2021). *Deepfakes. De juridische uitdagingen van de synthetische samenleving*. Tilburg University.
Smit, P.R. (2020). 'Nederland in internationaal perspectief'. In: R.F. Meijer, S.W. van den Braak & R. Choenni (Red.), *Criminaliteit en rechtshandhaving 2019* (p.105-109). Wetenschappelijk Onderzoek- en Documentatiecentrum.
Smit, S., A. de Vries, R. van der Kleij & H. van Vliet (2016). *Van predictive naar prescriptive policing. Meer dan vakjes voorspellen*. TNO.
Snaphaan, T. (2021). 'Licht, camera, actie! Een intelligencegestuurde aanpak van criminaliteit met crime scripting'. *Panopticon*, 42(6), p. 488-507.
Snaphaan, T., W. Hardyns & K. Ponnet (2020). 'AI in reductie van criminaliteit: een zwarte doos of de heilige graal?' In: J. de Bruyne & N. Bouteca (Red.), *Artificiële intelligentie en maatschappij* (p. 249-286). Gompel&Svacina.
Snaphaan, T., W. Hardyns, A. van Dijk, R. Spithoven & R. van Brakel (2023). 'Setting the scene. Big data policing als multidisciplinair thema voor praktijk, beleid en onderzoek'. In: T. Snaphaan, W. Hardyns, A. van Dijk, R. Spithoven & R. van Brakel (Eds.), *Big data policing* (p. 13-31). Gompel & Svacina.
Snaphaan, T., L.J.R. Pauwels & W. Hardyns (2023). 'Hypotheses non fingo? De rol van theoretische verklaringen in een bigdatatijdperk'. In: T. Snaphaan, W. Hardyns, A. van Dijk, R. Spithoven & R. van Brakel (Eds.), *Big data policing* (p. 33-52). Gompel & Svacina.
Snijders, D., M. Biesiot, G. Munnichs & R. van Est (2019). *Burgers en sensoren. Acht spelregels voor de inzet van sensoren voor veiligheid en leefbaarheid*. Rathenau Instituut.
Spapens, A.C.M. & D. van Mheen (2022). *Het vestigingsklimaat voor drugscriminaliteit in Nederland*. Tilburg University/Wetenschappelijk Onderzoek- en Documentatiecentrum.
Spithoven, R. & J. van de Pas (2020). 'Bij voorbaat effectiever? Over de noodzaak van herwaarderen van vakmanschap en de onvermijdelijkheid van actie-onderzoek bij het gebruik van big-datatoepassingen bij de politie'. In: W. Hardyns & T. Snaphaan (Eds.), *Big data & innovatieve methoden voor criminologisch onderzoek* (p. 131-147). Boom Criminologie.
Spithoven, R. (2020). *Verbonden risico's. Maatschappelijke veiligheid in de black box society*. Boom Criminologie.
Staring, R., L. Bisschop, R. Roks, E. Brein & H. van de Bunt (2019). *Drugscriminaliteit in de Rotterdamse haven: aard en aanpak van het fenomeen*. Erasmus School of Law.

Steden, R. van, R. Anholt & R. Koetsier (2021). *De kracht van gebiedsgebonden politiewerk. Een internationale literatuurstudie*. Politie Nederland/Vrije Universiteit Amsterdam/NSCR.
Stephenson, D. (2018). *Big data ontrafeld. Neem betere zakelijke beslissingen met big data, data science en AI*. Van Duuren Management.
Stevens, L. (2023). 'De inzet van identificerende gezichtsherkenningstechnologie in de publieke ruimte: vragen die moeten worden gesteld'. *Delikt en Delinkwent*, *50*(2), p. 1-6.
Stevens, L., M. Hirsch Ballin, M. Galič, S.S. Buisman, B. Groothoff, Y. Hamelzky, C. Lucas, K. Rasul & S. Verijdt (2021). '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*, *4*, p. 234-245.
Stichting Maatschappij en Veiligheid (2022). *Jong ontspoord in het drugsmilieu. En wat wij als samenleving daar tegenover moeten zetten*. SMV.
Stol, W.P. (1996). *Politie-optreden en informatietechnologie. Over sociale controle van politiemensen*. Koninklijke Vermande.
Stol, W.P. (2020). 'Digitalisering en criminaliteit. Een beknopte inleiding op cybercrime'. In: C. de Poot, E. Lievens, W.P. Stol & L. de Kimpe (Eds.), *Politie en cybercrime* (p. 13-22). Gompel & Svacina.
Stol, W.P. (2021). 'Digitalisering en de maatschappelijke rol van de politie. Naar politie als "autoriteit fatsoenlijke rechtshandhaving"'. In: G. Meershoek, J. Nap & L. van Spijk (Red.), *In naam der wat? Reflecties op politie en politiewerk* (p. 29-38). Boom Criminologie.
Stol, W.P. & L. Strikwerda (2017). *Strafrechtpleging in een digitale samenleving*. Boom Juridisch.
Stol, W.P. & L. Strikwerda (2018). 'Online vergaren van informatie voor opsporingsonderzoek. Een beknopte evaluatie van voorgestelde wetgeving'. *Tijdschrift voor Veiligheid,* 17(1-2), p. 8-22.
Stolze, J. (2018). *Algoritmisering, wen er maar aan! Leven, werken en geld verdienen met kunstmatige intelligentie*. Boom.
Susskind, J. (2022). *The digital republic. On freedom and democracy in the 21ste century*. Bloomsbury Publishing.
Swinkels, M. & L. van Zwieten (2022). 'Innovatieve cybercriminelen. De toepassing van de Book of Crime-methode door het Openbaar Ministerie en zijn partners'. In: A. van Dijk, P. de Baets, L. Gunther Moor, E. Devroe & S. Zouridis (Eds.), *Politie en rechtsstaat in de gedigitaliseerde samenleving* (p. 131-139). Gompel & Svacina.

Taylor Parkins-Ozephius, C.M., I.N. de Wit, D.A.G. van Toor & T. Beekhuis (2021). 'De politie als winkelier van smartphones met 'versleutelde' communicatiemiddelen: de inzet van de opsporingshandelingen getoetst aan het legaliteitsbeginsel'. *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, *5*, p. 322-333.
Tazelaar, P. (2017). 'IGP en ethiek, oftewel: wat mag wel en wat mag niet'. In: M. den Hengst, T. ten Brink & J. ter Mors (Red.), *Informatiegestuurd politiewerk in de praktijk* (p. 93-101). Vakmedianet.

Tegmark, M. (2017). *Life 3.0. Being human in the age of artificial intelligence*. Penguin Random House.
Terpstra, J. (2010a). *De maatschappelijke opdracht van de politie. Over identiteit en kernelementen van politiewerk*. Boom Juridische Uitgevers.
Terpstra, J. (2010b). *Het veiligheidscomplex. Ontwikkelingen, strategieën en verantwoordelijkheden in de veiligheidszorg*. Boom Juridische Uitgevers.
Terpstra, J. (2019). *Wijkagenten en veranderingen in hun dagelijks werk. Verslag van een onderzoek*. Sdu Uitgevers.
Terpstra, J., N.R. Fyfe & R. Salet (2019). 'The abstract police: a conceptual exploration of unintended changes of police organisations'. *The Police Journal*, *92*(4), p. 339-359.
Terpstra, J. & R. Salet (2018). 'De abstracte politie'. *Het Tijdschrift voor de Politie*, 80(5), 42-46.
Terpstra, J. & R. Salet (2020). 'Big data policing als sociale praktijk'. In: J. Janssens, W. Broer, M. Crispel & R. Salet (Eds.), *Informatiegestuurde politie* (p. 25-38). Gompel & Svacina.
Terpstra, J. & R. Salet (2023). 'Het einde van PredPol, het einde van predictive policing? Cahiers big data'. In: T. Snaphaan, W. Hardyns, A. van Dijk, R. Spithoven & R. van Brakel (Eds.), *Big data policing* (p. 209-216). Gompel & Svacina.
Terpstra, J., R. Salet, I. van Duijneveldt & T. Havinga (2021). *Gebiedsgebonden politiewerk in ontwikkeling. Onderzoek naar basisteams in een digitale en superdiverse samenleving*. Sdu Uitgevers.
Testerink, B., E. Nieuwenhuizen & F. Bex (2023). '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). Gompel & Svacina.
Thamm, A., M. Gramlich & A. Borek (2020). *The ultimate data and AI guide. 150 FAQs about artificial intelligence, machine learning and data*. Data AI GmbH.
Tops, P. (2022). *Ondermijning en datawetenschap: waar gaat dat over?* Tilburg University.
Tops, P. & J. Tromp (2017). *De achterkant van Nederland. Hoe onder- en bovenwereld verstrengeld raken*. Uitgeverij Balans.
Tops, P. & J. Tromp (2020). *Nederland drugsland. De lokroep van het geweld, de macht van criminelen, de noodzaak die te breken (en hoe dat dan te doen)*. Balans.
Torre, E. van der, A. van Wijk, M. Heijkoop, H. de Boer & J. Wolsink (2021). *Mainport in de tweede linie. Over sierteelt en ondermijning*. Bureau Beke.
Trottier, D. (2015). 'Coming to terms with social media monitoring: uptake and early assessment'. *Crime Media Culture*, 11(3), p. 317-333.
Trottier, D. & C. Fuchs (2015). 'Theorising social media, politics and the state: an introduction'. In: D. Trottier & C. Fuchs (Eds.), *Social media, politics and the state. Protests, revolutions, riots, crime and policing in the age of Facebook, Twitter and YouTube* (p. 3-38). Routledge.

Tundis, A. & M. Mühlhäuser (2020). 'The role of information and communication technology (ICT) in modern criminal organizations'. In; V. Ruggiero (Eds.), *Organized crime and terrorist networks* (p. 60-78). Routledge.
Tuptuk, N. & S. Hailes (2019). 'Crime in the age of the Internet of Things'. In: R. Wortley, A. Sidebottom, N. Tilley & G. Laycock (Eds.), *Routledge handbook of crime science* (p. 288-308). Routledge.
Turkle, S. (2021). *The empathy diaries. A memoir*. Penguin Press.
Tweede Kamer der Staten-Generaal (2020). *Ongekend onrecht. Verslag Parlementaire ondervragingscommissie Kinderopvangtoeslag*.

Valkenhoef, J. van, N. de Groes & P. Tops (2022). 'Drugshandel via poststukken vanuit Nederland'. In: A. van Dijk, P. de Baets, L. Gunther Moor, E. Devroe & S. Zouridis (Eds.), *Politie en rechtsstaat in de gedigitaliseerde samenleving* (p. 83-102). Gompel & Svacina.
Veen, H. ter & N. Kop (2021). *Innovatiekracht versterken. Een longitudinale processtudie naar technologisch innoveren bij de politie 2017-2020*. Politieacademie.
Veldhuizen, A. van (2023). Begrijpen voor ingrijpen. Op zoek naar een kennisgedreven politie. In: J. van Hoorn & M. van Bavel (Red.), *Onze politie in een kwetsbare rechtstaat* (p. 161-173). Gompel&Svacina.
Verhoeven, K. (2023). *De democratie crasht. Politieke onmacht in het digitale tijdperk*. Uitgeverij Business Contact.
Verlaan, D. (2020). *Ik weet je wachtwoord. Waargebeurde verhalen over de duistere kant van het internet*. Das Mag.
Vermeulen, I., M. Soudijn & W. van der Leest (2021). 'Open heimelijke netwerken in de Nederlandstalige georganiseerde synthetische-drugscriminaliteit'. *Tijdschrift voor Criminologie*, *63*(2), p. 187-211.
Versteegh, P., T. van der Plas & H. Nieuwstraten (2011). *The best of three worlds. Effectiever politiewerk door een probleemgerichte aanpak van hot crimes, hot spots, hot shots en hot groups*. Politieacademie.
Vestby, A. & J. Vestby (2019). 'Machine learning and the police: asking the right questions'. *Policing: A Journal of Policy and Practice*, *15*(1), p. 44-58.
Vetzo, M. & J.H. Gerards (2019). 'Algoritme-gedreven technologieën en grondrechten'. *Computerrecht*, 3(1), p. 10-19.
Vis, T. (2012). *Intelligence, politie en veiligheidsdienst: Verenigbare grootheden?* Tilburg University.
Vliet. H. van, C. Bonte, R. Schipper & P. van Dusseldorp (2019). *Smart cities en stedelijke veiligheid. Slim delen en samen leren*. The Hague Security Delta.
Volberda, H., K. Heij & M. Bosma (2019). *Innovatie. Jij. Nu. Niet de robots maar wij zijn aan zet*. Managementimpact.
Voort, N. van der & W.M. Warnaars (2020). 'Cybersecurity anno 2020. Het is niet de vraag of je wordt gehackt, maar wanneer'. *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 5, p. 253-259.

Vries, A. de, M. Menkhorst, H. van Vliet, H. Stavleu, C. Bonte & C. Schilder (2018). *Wie kijkt er mee? Het nieuwe melden. De impact van beeld*. TNO.
Vries, G.M. de, J. Bijlsma, A-R. Mackor, G. Meynen & F. Bex (2021). 'AI-risicotaxatie: nieuwe kansen en risico's voor statistische voorspellingen van recidive'. *Boom Strafblad*, 2, p. 58-66.
Vries, I. de (2017). 'Big data'. In: M. den Hengst, T. ten Brink & J. ter Mors (Red.), *Informatiegestuurd politiewerk in de praktijk* (p. 249-262). Vakmedianet.

Waard, J. de (2020). *Ontwikkelingen in de (geregistreerde) criminaliteit. Nationale en internationale trends en verklaringen*. Ministerie van Justitie & Veiligheid.
Waardenburg, L. (2021). *Behind the scenes of artificial intelligence. Studying how organizations cope with machine learning in practice*. Haveka.
Waardenburg, L., M. Huysman & M. Agterberg (2020). *S.L.I.M. managen van AI in de praktijk. Hoe organisaties slimme technologie implementeren*. Mediawerf.
Waardenburg, L., A. Sergeeva & M. Huysman (2020). 'Predictive policing ontcijferd. Een etnografie van het "Criminaliteits Anticipatie Systeem" in de praktijk'. In: J. Janssens, W. Broer, M. Crispel & R. Salet (Eds.), *Informatiegestuurde politie* (p. 69-88). Gompel & Svacina.
Wagen, W. van der (2018). *From cybercrime to cyborg crime: An exploration of high-tech cybercrime, offenders and victims through the lens of actor-network theory*. Rijksuniversiteit Groningen.
Wagen, W. van der, J.J. Oerlemans & M. Weulen Kranenbarg (2020a). 'Inleiding'. In: W. van der Wagen, J.J. Oerlemans & M. Weulen Kranenbarg (Red.), *Basisboek cybercriminaliteit. Een criminologisch overzicht voor studie en praktijk* (p.13-19). Boom Criminologie.
Wagen, W. van der, J.J. Oerlemans & M. Weulen Kranenbarg (2020b). 'Cybercriminaliteit in criminologisch perspectief'. In: W. van der Wagen, J.J. Oerlemans & M. Weulen Kranenbarg (Red.), *Basisboek cybercriminaliteit. Een criminologisch overzicht voor studie en praktijk* (p. 21-53). Boom Criminologie.
Wall, D.S. (2007). *Cybercrime. The transformation of crime in the information age*. Polity Press.
Weerd, C. van & D. Lassche (2021). *National security implications of quantum technology and biotechnology*. HCSS/TNO.
Weijer, S.G.A. van de & E.R. Leukfeldt (2023). *Cybercriminaliteit tijdens de coronacrisis: aard, omvang en impact van cyberrisico's voor burgers en het MKB*. Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving/Haagse Hogeschool.
Weijer, S.G.A. van de, E.R. Leukfeldt & S. van der Zee (2020). *Een onderzoek naar aangiftebereidheid onder burgers en ondernemers*. Sdu Uitgevers.
Weijers, I., H. Ferwerda & R. Roks (2021). 'Te groot voor de wijkagent, te klein voor de recherche. Een vergeten groep: jonge doorgroeiers in de criminaliteit'. *Proces*, 100(5), p. 264-275.
Welten, J.A.M., A.J. van, Dijk, A.M. de Bruin, F.C. Hoogewoning, G.F.S.J. Kuijlaars, L.O. Luinenburg, D. Roest & R.R.H. van Zeijst (2019). *Politiefunctie en rechtsstaat in de*

gedigitaliseerde samenleving. Positionering in een meervoudige context. Politie Nederland.
Werdmölder, H. (2022). *Nederland narcostaat. Na 50 jaar drugshandel en talloze liquidaties*. Just Publishers.
Wessels, M. (2023). 'Algorithmic policing accountability: eight sociotechnical challenges'. *Policing and Society*, DOI: 10.1080/10439463.2023.2241965
Wetenschappelijke Raad voor het Regeringsbeleid (2015). *De publieke kern van het internet. Naar een buitenlands internetbeleid*. Amsterdam University Press.
Wetenschappelijke Raad voor het Regeringsbeleid (2016). *Big data in een vrije en veilige samenleving*. Amsterdam University Press.
Wetenschappelijke Raad voor het Regeringsbeleid (2021a). *Opgave AI. De nieuwe systeemtechnologie*. Amsterdam University Press.
Wetenschappelijke Raad voor het Regeringsbeleid (2021b). *Politiefunctie in een veranderende omgeving*. WRR.
Weulen Kranenbarg, M. (2018). *Cyber-offenders versus traditional offenders. An empirical comparison*. Vrije Universiteit Amsterdam.
Weulen Kranenbarg, M., Y. van der Toolen & F. Weerman (2022). *Understanding cybercriminal behaviour among young people. Results from a longitudinal network study among a relatively high-risk sample*. Nederlands Studiecentrum Criminaliteit en Rechtshandhaving/Vrije Universiteit Amsterdam.
Wieland, F. (2022). 'Veiligheid regisseren in de sensorsamenleving'. *Het Tijdschrift voor de Politie*, 84(3), p. 30-34.
Wientjes, J., M. Delsing, A. Cillessen, J. Janssens & R. Scholte (2017). 'Identifying potential offenders on the basis of police records: development and validation of the ProKid risk assessment tool'. *Journal of Criminological Research, Policy and Practice*, 3(4), p. 249-260.
Wijk, A. van, I. van Leiden & M. Hardeman (2017). *De modus operandi van de recherche. De rechercheprakti jk in moord- en verkrachtingszaken*. Reed Business.
Wijngaarden, M. van & R. Schiffelers (2023). 'Internet vraagt een andere politie'. *Het Tijdschrift voor de Politie*, 85(2), p. 6-9.
Williamson, T. (2008). *The handbook of knowledge-based policing. Current conceptions and future directions*. John Wiley & Sons.
Willis, J.J., C.S. Koper & C. Lum (2022). 'An assessment of police technology and the "iron cage" of the abstract police in the United States'. In: J. Terpstra, R. Salet & N.R. Fyfe (Eds.), *The abstract police. Critical reflections on contemporary change in police organisations* (p. 151-168). Eleven.
Wilson, D. (2018). 'Algorithmic patrol: the futures of predictive policing'. In: A. Završnik (Eds.), *Big data, crime and social control* (p. 108-127). Routledge.
Wilson, D. (2019). 'Platform policing and the real-time cop'. *Surveillance & Society*, 17(1/2), p. 69-75.
Wilson-Kovacs, D. (2021). 'Digital media investigators. Challenges and opportunities in the use of digital forensics in police investigations in England and Wales'. *Policing: An International Journal*, 44(4), 669-682.

Winter, H., J. Bekkering, T. Floor, B. Geertsema, S. Roest & J. Smits (2020*). De verwerking van politiegegevens in vijf Europese landen*. Rijksuniversiteit Groningen.
Winters, T. (2021). *The metaverse. Prepare now for the next big thing*. Independently Published.
Wit, B. de (2021). *Society 4.0. Resolving eight key issues to build a citizens society*. Vakmedianet.

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

Završnik, A. (2018). 'Big data: what is it and why does it matter for crime and social control'. In: A. Završnik (Eds.) *Big data, crime and social control* (p. 3-28). Routledge.
Zedner, L. (2007). 'Pre-crime and post-criminology?' *Theoretical Criminology*, 11(2), p. 261-281.
Zouridis, S. (2019). *De institutionele crisis van de rechtsstaat. Over de binnenkant van rechtsstatelijk bestuur*. Boom Bestuurskunde.
Zouridis, S., M. van Eck & M.A.P. Bovens (2019). 'Automated discretion'. In; T. Evans & P. Hupe (Eds.), *Discretion and the quest for controlled freedom* (p. 313-329). Palgrave Macmillan.
Zuboff, S. (2019). *The age of surveillance capitalism. The fight for the future at the new frontier of power*. Profile Books.
Zuidberg, M.C., L.C. Schreuders, H.C. Tops & A.A. Mapes (2018). *Eindrapportage DNASuccesmeter*. Amsterdam University of Applied Sciences.
Zuurveen, R. & W.P. Stol (2020). *Benutten van digitale sporen*. Sdu Uitgevers.

Leden Redactieraad Programma Politie & Wetenschap

Voorzitter	prof. em. dr. ir. J.B. Terpstra Radboud Universiteit Nijmegen
Leden	mr. drs. C. Bangma Politie, Eenheid Midden-Nederland
	mw. mr. W.M. de Jongste Projectbegeleider Wetenschappelijk Onderzoek- en Documentatiecentrum Ministerie van Justitie en Veiligheid
	dr. P.P.H.M. Klerks Raadadviseur Parket-Generaal, Openbaar Ministerie
	mr. drs. C. Loef Adviseur Gemeente Amsterdam
	mw. J. Overeem Politie, Eenheid Midden-Nederland
	prof. em. dr. P. van Reenen Van Reenen-Russel Consultancy b.v. Studie- en Informatiecentrum Mensenrechten (SIM) Universiteit Utrecht
Secretariaat	Programmabureau Politie & Wetenschap Politieonderwijsraad Koninginnegracht 62 2514 AG Den Haag
	Postbus 25842 2502 HV Den Haag www.politieenwetenschap.nl