



NIEUWE TECHNOLOGIE, OUDE ONRECHT- VAARDIGHEID.

OP DATA GEBASEERDE DISCRIMINATIE
EN CRIMINALISERING BIJ DE POLITIE
EN IN GEVANGENISSEN IN EUROPA

GESCHREVEN DOOR:

Griff Ferris

Sofia Lyall

GEFINANCIERD DOOR:

European
Artificial Intelligence
& Society Fund

Informatie over de publicatie

Auteurs: Griff Ferris, Sofia Lyall

Uitgever: Chris Jones

Ontwerp: McKensie Marie

Dit rapport kreeg steun van de European AI & Society Foundation.

Gepubliceerd door Statewatch, juni 2025.

About Statewatch

Statewatch voert kritisch onderzoek, beleidsanalyse en onderzoeksjournalistiek uit en promoot dit om debatten, bewegingen en campagnes voor burgerlijke vrijheden, mensenrechten en democratische normen van informatie te voorzien. We zijn actief sinds 1991 en zijn gevestigd in Londen.

statewatch.org

(+44) (0) 203 393 8366

**MayDay Rooms, 88 Fleet Street, London
EC4Y 1DH, UK**

Steun ons werk

U kan ons werk steunen via giften:



Inschrijven op onze nieuwsbrief:

— [Zich aanmelden](#)

**Ingeschreven als liefdadigheidsinstelling in
het VK onder nummer: 1154784**

**Ingeschreven in het VK onder
ondernemingsnummer: 08480724**

**Officiële Ondernemingsnaam: The
Libertarian Research & Education Trust**

**Maatschappelijke zetel: 88 Fleet Street,
London EC4Y 1DH, UK.**

Inhoud

Dankwoord	4
Definities	5
Samenvatting	12
Inleiding	12
Op locatie gebaseerde ‘voorspellende’ systemen	23
Op individuen gerichte systemen om criminaliteit te ‘voorspellen’ en te profileren	38
Videobewakingssystemen met AI	49
Databanken	53
Conclusie	57
Beeldkredieten	64
Eindnoten	65

Dankwoord

Dit werk werd mogelijk gemaakt door onderzoekers en partnerorganisaties in België, Frankrijk, Duitsland en Spanje:

- België: Corentin Debailleul, Technopolicy België en Ligue des droits humains;
- Frankrijk: Edlira Nano en Félix Tréguer, La Quadrature du Net, met steun van de leden van de werkgroep Technopolicy Frankrijk van La Quadrature du Net;
- Duitsland: Sonja Peteranderl, AlgorithmWatch;
- Spanje: Naiara Bellio, met medewerkers Ana Valdivia en Javier Sánchez Monedero, AlgoRace.

Wij bedanken alle mensen en groepen die deelgenomen hebben aan interviews of op een andere manier informatie, ervaringen of expertise gedeeld hebben.

We willen ook de mensen en organisaties bedanken die racisme en discriminatie bij de politie en in rechtsstelsels, wat door deze nieuwe technologieën gewoon gereproduceerd wordt, in vraag stellen en er stappen tegen ondernemen.

Definities

Artificiële intelligentie

De Verordening Artificiële intelligentie van de EU definieert een Ai-systeem als volgt:

“...een op een machine gebaseerd systeem dat is ontworpen om met verschillende niveaus van autonomie te werken en dat na het inzetten ervan aanpassingsvermogen kan vertonen, en dat, voor expliciete of impliciete doelstellingen, uit de ontvangen input afleidt hoe output te genereren zoals voorspellingen, inhoud, aanbevelingen of beslissingen die van invloed kunnen zijn op fysieke of virtuele omgevingen;”¹

Dit rapport gebruikt deze definitie, hoewel er vele manieren zijn om AI en AI-systemen te definiëren.² Het is belangrijk om op te merken dat de meest op data gebaseerde, algoritmische en geautomatiseerde systemen die de politie en de strafrechtelijke autoriteiten in Europa gebruiken geen artificiële intelligentie gebruiken. Sommige systemen gebruiken machinaal lerende systemen (cf. Infra), een subveld van AI. De meeste systemen gebruiken echter klassieke statistische methoden en kunnen beschreven worden als geautomatiseerde besluitvormingssystemen (cf. infra).

Geautomatiseerd besluitvormingssysteem

Het Kantoor voor AI van het Verenigd Koninkrijk definieert automatische besluitvormingssystemen als systemen die “enkel geautomatiseerde beslissingen gebruiken (geen menselijk oordeel) en “geautomatiseerde ondersteunende besluitvorming (als ondersteuning van menselijk oordeel).”³

Machinaal lerend

De Cambridge Dictionary definieert machinaal lerend als “het proces waarbij computers hun eigen vermogen om taken uit te voeren analyseren, zonder dat een mens instructies hoeft te geven in de vorm van een programma, of de studie van het maken en gebruiken van computersystemen die dit kunnen doen.”⁴

‘Predictive’ policing:

Er zijn twee belangrijke vormen van wat ‘predictive policing’ genoemd wordt: gebaseerd op locaties en gebaseerd op personen. Amnesty International definieert systemen voor predictive policing als volgt:

... Computerprogramma's die data en algoritmische modellen gebruiken om het

risico in te schatten dat een misdaad zal worden gepleegd. Systemen voor predictive policing berekenen risicoscores die zogenaamd het risico weergeven dat een persoon of een groep personen het slachtoffer of de dader wordt (op personen gebaseerde predictive policing) of dat een bepaalde plek de plaats van een delict zal worden (op locatie gebaseerde predictive policing). De politie treft dan maatregelen op basis van deze door de computer gegenereerde risicoscores om de voorspelde misdaad te voorkomen of op te sporen door de activiteiten van de politie te richten op plekken, individuen of groepen die beschouwd worden als een ‘hoog risico’.’¹⁵





Samenvatting

De politie en strafrechtelijke autoriteiten in Europe gebruiken steeds meer op data gebaseerde systemen en instrumenten om te ‘voorspellen’ waar er misdrijven zullen plaatsvinden, om mensen als criminelen te profileren en het ‘risico’ op een misdaad of op criminaliteit in de toekomst te beoordelen.

Deze zogenaamde ‘voorspellingen’, profielen en risicobeoordelingen hebben een impact op de beslissingen, acties en interventies van de politie. Dit omvat toezicht en monitoring, ondervraging, fouilleren, identiteitscontroles, uitsluiting van werkgelegenheid, huiszoekingen, boetes, gebruik van geweld, detentie, arrestatie en uitzetting.

Deze op data gebaseerde systemen en beslissingen beïnvloeden ook keuzes binnen het strafrechtelijke systeem: van hechtenis en voorlopige hechtenis tot vervolging, veroordeling en reclassering.

Buiten het strafrechtelijke systeem kunnen geautomatiseerde beslissingen ook leiden tot andere vormen van bestraffing of er een invloed op hebben. Zo kunnen ze ten grondslag liggen aan het weigeren of beperken van toegang tot essentiële publieke diensten, zoals sociale bijstand of huisvesting.

Dit rapport bundelt origineel onderzoek over geautomatiseerde besluitvormingssystemen en databanken die gebruikt worden in het politiewerk en het strafrechtelijk systeem in vier landen: België, Frankrijk, Duitsland en Spanje. Het is gebaseerd op diepgaand

onderzoek van partnerorganisaties in deze landen.⁶ Het kijkt specifiek naar:

- Hoe op data gebaseerde systemen voor voorspelling van misdaad ontwikkeld worden;
- Hoe ze gebruikt worden door wetshandhaving en strafrechtelijke autoriteiten;
- De outputs van deze systemen;
- Hoe deze outputs gebruikt worden en beslissingen beïnvloeden en de impact die ze hebben op mensen, groepen en gemeenschappen.

Het bekijkt ook hoe deze systemen onevenredig gericht zijn en een impact hebben op gemarginaliseerde groepen en gemeenschappen, inclusief zwarte en geracialiseerde mensen en gemeenschappen, slachtoffers van gendergebaseerd geweld, migranten en mensen uit de arbeidersklasse en sociaal achtergestelde milieus en gebieden en mensen met geestelijke gezondheidsproblemen.

De meeste systemen gebruiken historische gegevens, bijvoorbeeld van politiesystemen of het strafrechtelijke systeem. Dit is een weerspiegeling van historische en bestaande vooroordelen binnen deze instellingen en de maatschappij in het algemeen. Dit leidt tot overdreven aanwezigheid van politie en criminalisering van gemarginaliseerde gemeenschappen, vooral geracialiseerde groepen, migranten en mensen uit armere buurten.

Het gebruik van deze systemen in politiewerk en het strafrechtelijke systeem heeft aanzienlijke gevolgen voor de rechten van individuen, inclusief het recht op een eerlijk proces en vrijwaring van discriminatie.

Op locatie gebaseerde predictive policing-systemen

Politiekorpsen in heel Europa ontwikkelen op locatie gebaseerde methoden voor ‘predictive’ policing en voeren ze in. Deze algoritmische systemen worden ontwikkeld om te ‘voorspellen’ waar en wanneer er een misdaad gepleegd zal worden. Zo kan de politie mankrachten aan deze locaties toewijzen. Geografische systemen om



misdaad te ‘voorspellen’ worden of werden in alle vier bestudeerde landen gebruikt, namelijk België, Frankrijk, Duitsland en Spanje, maar ook in andere Europese landen zoals bijvoorbeeld Italië, Nederland, Zwitserland en het VK.

Het onderzoek heeft de twee belangrijkste soorten op locatie gebaseerde systemen geïdentificeerd:

- Voorspelling van ‘hotspots’ van misdaad, waarbij historische politiegegevens gebruikt worden om plaatsen waar in de toekomst misdrijven gepleegd zullen worden te voorspellen; en
- Algoritmes voor een op omgeving gebaseerde voorspelling van risico, gebaseerd op de veronderstelling dat omgevingsfactoren bepalen waar misdaden gepleegd worden. Ze zouden dus ‘risicolocaties’ kunnen voorspellen.

Methodes om ‘hotspots’ voor criminaliteit te voorspellen gebruiken historische statistische gegevens rond misdaad over waar en wanneer misdaden bedreven werden om zo de locaties van criminaliteit, oftewel ‘hotspots’, te ‘voorspellen’. Deze voorspellingen zijn gebaseerd op de analyse van statistische inzichten en trends in grote hoeveelheid gegevens over criminaliteit, vaak uit databanken van de politie. In het algemeen geven deze systemen om ‘hotspots’ te voorspellen de politie een heatmap om gebieden of locaties te identificeren waar er een hoog risico op misdaad zou zijn.

Deze systemen om ‘hotspots’ voor criminaliteit te voorspellen worden gebruikt om de middelen van de politie toe te wijzen en te bepalen waar en wanneer politieagenten patrouilles uitvoeren. Uitkomsten in gebieden die ‘hotspot’ zouden zijn, zijn onder andere toezicht, informatievergaring, identiteitscontroles, ondervraging, fouilleringen, straatverboden, huiszoekingen en arrestaties. Het onderzoek uit bezorgdheid over het feit dat locaties die als ‘hotspots’ voor criminaliteit worden bestempeld in onevenredige mate gebieden of buurten zijn waar mensen met een laag inkomen en geracialiseerde gemeenschappen wonen en werken.

Op locatie gebaseerde systemen zijn gebaseerd op omgevings- en contextuele gegevens. Ze maken gebruik van omgevings- en contextuele gegevens om gebieden of locaties te identificeren die naar verluidt gevoeliger zijn voor criminaliteit. Een algoritme kent



een bepaalde gevoeligheidswaarde toe aan locaties op basis van ruimtelijke factoren zoals:

- of de locatie goed verlicht is;
- metro- en busstations;
- ruimtes om buiten te zitten of cafés;
- fastfoodrestaurants;
- openbare toiletten;
- apotheken, bars, bepaalde soorten winkels;
- bomen en banken; en
- scholen en postkantoren.

Deze methode roept vragen op rond vooroordelen en discriminatie, net zoals bij systemen gebaseerd op gegevens rond criminaliteit.

Op personen gerichte ‘predictive’ policing en systemen om criminaliteit te ‘voorspellen’

Op personen gerichte tools om criminaliteit te ‘voorspellen’ zijn bedoeld om te voorspellen hoe waarschijnlijk het is of welk risico er bestaat dat deze persoon een misdaad zou plegen. Er worden gelijkaardige systemen aangewend om te beoordelen hoe waarschijnlijk het is dat iemand een slachtoffer wordt van een misdaad, zoals gendergebaseerd geweld, of om zogenaamde valse aangiftes van misdaad op te sporen.

De gegevens van de mensen waarop deze systemen zich richten, worden voortdurend geanalyseerd: hun leven in het verleden en het heden en hun relaties. Het doel is om hun gedrag, het ‘risico’ dat ze inhouden of hun veronderstelde ‘criminaliteit’ te bepalen en ‘voorspellen’. Dit kan ernstige gevolgen hebben. De resultaten die deze systemen opleveren, kunnen ervoor zorgen dat mensen onder constant toezicht of monitoring staan. Dit kan leiden tot een toename in politiecontroles, ondervragingen, fouilleringen, bezoeken aan huis of op het werk, uitsluiting van werkgelegenheid, detentie, uitzetting of arrestatie.

Deze tools worden ook in het strafrechtelijke systeem gebruikt



en kunnen een invloed hebben op besluitvorming van rechters, inclusief veroordeling. Dit kan een invloed hebben op de lengte van de gevangenisstraf, wanneer de persoon vrijkomt en de omstandigheden waarin ze aangehouden blijven.

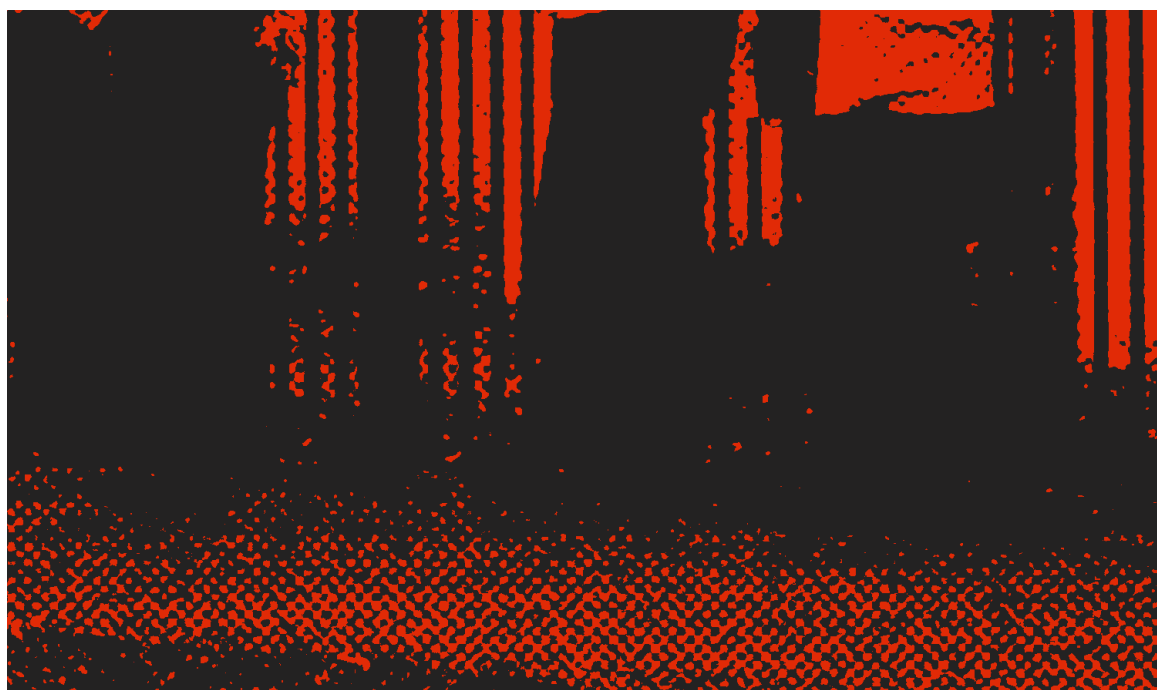
Conclusie

Het gebruik van deze systemen leidt tot raciale en socio-economische profilering, discriminatie en criminalisering. Het is vooral gericht tegen gemarginaliseerde mensen en gemeenschappen, vooral zwarte en als minderheden behandelde ethniciteiten en mensen uit achtergestelde milieus.

Het gebruik heeft onrechtvaardige en discriminerende gevolgen: van toezicht, identiteitscontroles en fouilleringen tot pesterijen door de politie, huiszoekingen, uitsluiting van werkgelegenheid, arrestatie, detentie en deportatie.

Deze systemen worden heimelijk gebruikt. Dit betekent dat mensen zich niet van het gebruik bewust zijn. Het resultaat is dat de mensen waarop deze systemen zich richten en de handelingen die er het gevolg van zijn, niet kunnen bevragen. Zelfs wanneer ze er zich wel bewust van zouden zijn, zou dat niet kunnen aangezien er geen duidelijk kader voor verantwoording is.

De conclusie van alle verslagen van partners en van dit rapport is dezelfde: deze systemen moeten worden verboden.





Inleiding

In heel Europa gebruiken de politie en de strafrechtelijke autoriteiten een grotere waaier aan digitale en op data gebaseerde systemen. Er worden aan een duizelingwekkend tempo nieuwe systemen ingevoerd, met weinig transparantie over de invoering of voorafgaande overwegingen van hun effecten en gevolgen.

Deze systemen omvatten:

- toezicht via gezichtsherkenning;
- systemen die emoties herkennen;
- extractietools voor smartphones;
- elektronische tags en monitoring via enkelband; en
- ‘voorspellende’ en profilerende systemen.

Wat deze praktijken gemeenschappelijk hebben, is het verzamelen en verwerken van enorme hoeveelheden gegevens, vaak gevoelige persoonsgegevens, om op basis daarvan beslissingen te nemen.

Dit rapport behandelt vooral op data gebaseerde, algoritmische en geautomatiseerd besluitvormingssystemen die de politie gebruikt om te ‘voorspellen’ waar en

wanneer misdaden gepleegd zullen worden en door wie. Voorstanders van deze zogenaamd wetenschappelijke en ‘voorspellende’ methodes halen als argument aan dat de politie hiermee efficiënter kan werken en tegelijkertijd kosten kan besparen:

“Door een nieuwe strategie, namelijk ‘op bewijs gebaseerd politiewerk’ te gebruiken, kunnen regeringen transparant samenwerken met de politie en het publiek om in kostenefficiënt politiewerk te investeren. Deze investeringen kunnen uitgevoerd worden terwijl het budget voor de politie tegelijkertijd verminderd kan worden door dure maar niet-efficiënte politietaken een halt toe te roepen.”⁷

De coördinator voor AI van de Gendarmerie Nationale in Frankrijk, kolonel Patrick Perrot, beweerde dat op data gebaseerde methoden ervoor zorgen dat politie kan anticiperen op misdaden, voor ze gepleegd worden:

... Met de wetenschappelijke benadering kunnen we modelleringstechnieken ontwikkelen die ontwikkelingen in de toekomst kunnen begrijpen en voorbereiden. Het begrip anticipatie is van doorslaggevend belang op het vlak van criminaliteit.”⁸

Dit heeft op zijn beurt geleid tot toenemende kritiek vanuit het maatschappelijk middenveld en van politieke activisten, organisatoren en academici in heel Europa op zogenaamde ‘voorspellende’ politiesystemen.

Vele groepen hebben ernstige zorgen geuit over de mogelijke gevolgen van deze systemen (zoals toezicht, monitoring, ondervraging, fouilleringen, boetes, huiszoekingen, gebruik van geweld, uitzetting, detentie en arrestatie) en over de mogelijke schendingen van individuele rechten. Deze systemen hebben een impact op en schenden mogelijk het recht op een eerlijk proces, het recht op privacy, vrijwaring van discriminatie, het vermoeden van onschuld en het recht op een doeltreffend rechtsmiddel.⁹

Het in dit rapport gebundelde onderzoek doet deze bezorgdheid nog toenemen. Het wil campagnes ondersteunen die internationaal, nationaal, regionaal en lokaal gebeuren en die oproepen tot een verbod op het gebruik van AI en algoritmes door strafrechtelijke autoriteiten. Waar dergelijke verboden nog niet zijn ingevoerd, zijn procedurele waarborgen nodig, waaronder strenge tests vóór ingebruikname, vereisten op het gebied van publieke transparantie en daadwerkelijke mogelijkheden tot verhaal.



Grote lijnen van het rapport

Dit rapport bundelt diepgaand onderzoek naar ‘voorspellende’ systemen en databanken binnen de politiewerk en het strafrechtelijk systeem in Europa en vat het samen. Dit gebeurde op basis van onderzoek in vier landen: België, Frankrijk, Duitsland en Spanje.

Deze landen werden hoofdzakelijk om twee redenen gekozen. Het was bekend dat ‘voorspellende’ systemen op ruime schaal werden ingezet door politiediensten en binnen het strafrechtelijk systeem. Tegelijkertijd was er weinig openbaar toegankelijk onderzoek naar de ontwikkeling, het gebruik en de impact van deze systemen.

Dit onderzoek werd in de loop van 2023 en 2024 uitgevoerd door onderzoekers bij *AlgorithmWatch*, *La Quadrature du Net* en *Technopolice*. De originele versies zijn online terug te vinden.¹⁰ *AlgoRace* voerde extra onderzoek uit voor Spanje.

In elk land hebben onderzoekers ernaar gestreefd om de gebruikte ‘voorspellende’ systemen bloot te leggen en na te gaan hoe ze functioneren, wat de resultaten zijn en welke impact ze hebben op mensen, groepen en gemeenschappen.

Dit onderzoek werd in dit rapport gebundeld om een overzicht te geven van het landschap, de trends en gevolgen van ‘predictive’ policing in België, Frankrijk, Duitsland en Spanje. Het omvat ook ander onderzoek en andere rapporten over het gebruik van ‘voorspellende’ en profilerende systemen in politiewerk en strafrechtelijke systemen elders in Europa, zoals in Nederland, Italië, Nederland, Zwitserland en het VK.

Vier delen van dit rapport onderzoeken de op data gebaseerde ‘voorspellende’ systemen die de politie gebruikt: op locatie gebaseerde systemen, op het individu gebaseerde systemen, videotoezicht met AI en databanken. Elk deel brengt een aantal belangrijke voorbeelden uit alle landen samen en bespreekt de doelen, inputs van data en de resultaten van de systemen.

Het laatste deel van het rapport analyseert de belangrijkste bezorgdheden en inbreuken op rechten van individuen, inclusief discriminatie, criminalisering, transparantie, verantwoording en onrechtmatigheid.





Structurele en institutionele discriminatie

De meeste systemen om misdaden te ‘voorspellen’ gebruiken historische gegevens rond criminaliteit. Dit is een weerspiegeling van bestaand institutioneel racisme, discriminatie en vooroordelen binnen de politie en de strafrechtelijke instellingen en de maatschappij in het algemeen.

Slachtoffers, verenigingen voor slachtoffers, academici, mensenrechtenorganisatie en internationale organisaties bekritiseren de discriminerende politiepraktijken met raciale en etnische profilering al lang. Deze praktijken leiden tot mensen tegenhouden, identiteitscontrole en fouilleren op basis van geracialiseerde eigenschappen zoals huidskleur of (veronderstelde) religieuze overtuiging.

Uit een studie uit 2017 van het Bureau van de Europese Unie voor de grondrechten, waarbij mensen uit alle toenmalige lidstaten (28) bevestigd werden, bleek dat bijna de helft van de respondenten van bepaalde als minderheid beschouwde, etnische gemeenschappen door de politie tegengehouden werden. Dit waren mensen met een “herkomst uit Afrika ten zuiden van de Sahara” in Luxemburg en Finland, mensen met “Noord-Afrikaanse achtergrond” in Nederland en Roma in Griekenland en Portugal.¹¹

De meeste mensen van ‘Afrikaanse afkomst’ die in de EU door de politie tegengehouden werden, vonden dat dit raciaal gemotiveerd was, volgens het Bureau van de Europese Unie voor grondrechten.¹² In Frankrijk lopen jonge mannen die als zwart of Arabisch beschouwd worden 20 keer (2000%) meer kans om door de politie tegengehouden te worden dan de rest van de bevolking, volgens de Franse ombudsman voor mensenrechten.¹³

In België is er een gebrek aan officiële informatie over etnische profilering, aangezien het historisch gezien niet verplicht was voor de politie om een bestand bij te houden van de controles die ze uitvoeren. Amnesty International heeft echter Belgische politieagenten geïnterviewd die zelf toegaven dat raciale profilering in politiewerk een realiteit was. Een van hen zei: “Ik gebruik etnische profilering. Ik zou niet weten hoe ik mijn job anders zou moeten doen. We moeten discrimineren. Anders zouden we niemand betrappen.”¹⁴

De politie in Spanje houdt mensen onevenredig vaak tegen en fouilleert hen op basis van hun raciale, etnische of religieuze uiterlijk. Dit werd in talrijke studies aangetoond.¹⁵ Mensen uit Noord-Afrika, Afrika ten zuiden van de Sahara en Oost-Europese landen worden vaker ontworpen aan identiteitscontroles dan Spaanse mensen.¹⁶

In Duitsland zijn individuen met een buitenlandse nationaliteit oververtegenwoordigd bij de verdachten van de politie, bij veroordelingen in de rechtbanken en bij mensen die een gevangenisstraf uitzitten.¹⁷ In België kwam een studie tot de conclusie dat mensen in rechtszaken die een naam hadden die als moslim beschouwd werd, meer kans op veroordeling hadden dan mensen met een naam die als Belgisch beschouwd werd, wanneer er voor de rest geen verschillen waren.¹⁸ In Frankrijk hebben niet-Fransen drie keer meer kans om in voorlopige hechtenis gehouden te worden.¹⁹ In België is 45% van de mensen in voorlopige hechtenis geen Belgisch burger.²⁰

Ondanks dit duidelijke bewijs is discriminatie door de politie, wetshandhaving en het strafrechtelijke systeem nog niet ruim erkend of herkend als een structureel of institutioneel probleem in vele Europese landen. Zoals de zwarte auteurs van de Afrozensus 2020, een enquête bij 6000 zwarte en Afrikaanse mensen en mensen uit de Afrikaanse diaspora, aangeven:

“... Het grote publiek stelt zich nog de vraag of er echt institutioneel racisme is in de Duitse politie of of dit geïsoleerde gevallen zijn. Dit is niet het geval voor zwarte en Afrikaanse mensen en mensen uit de Afrikaanse diaspora. Voor hen is dat een realiteit.”²¹

Deze gegevens, die institutionele en systemische discriminatie weergeven, worden gebruikt in ‘voorspellende’ en profilerende systemen en systemen voor risicobeoordeling door wetshandhaving en strafrechtelijke autoriteiten.

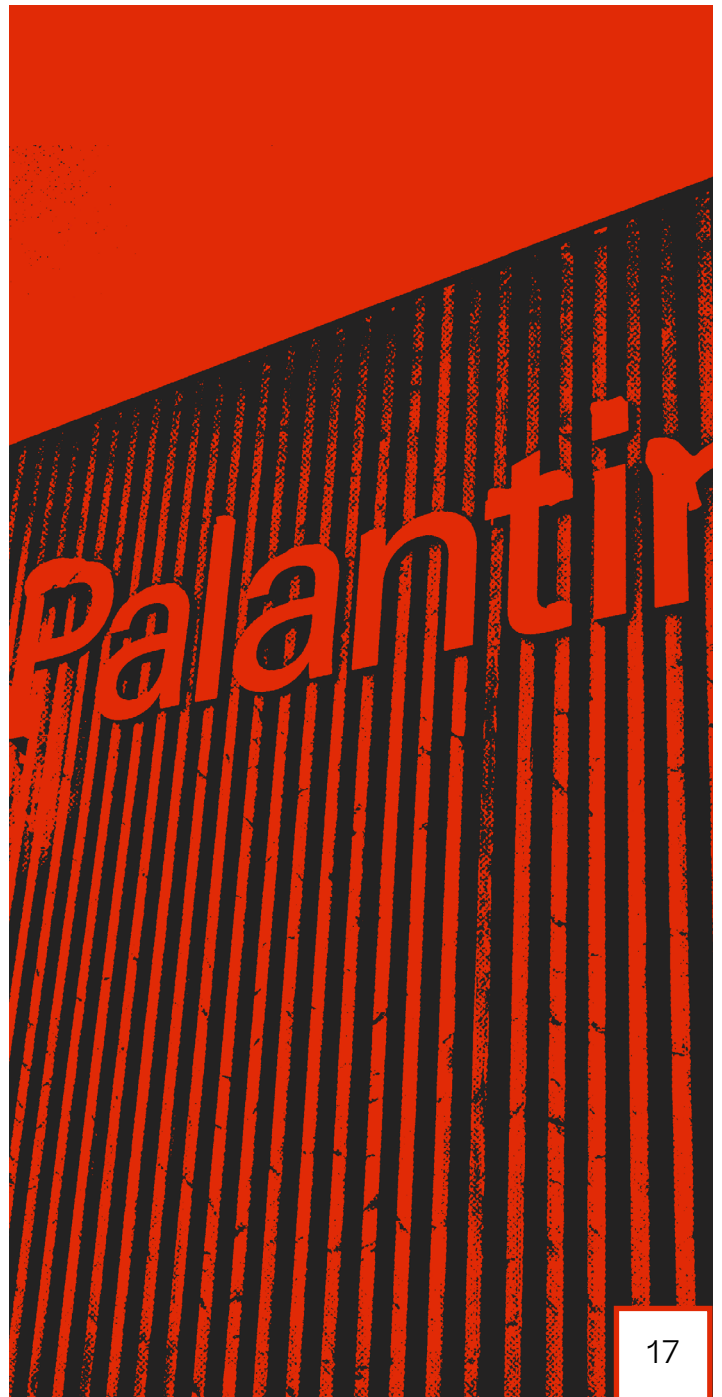
Betrokkenheid van het bedrijfsleven

Particuliere bedrijven zijn belangrijke spelers in de digitalisering en automatisering van politiewerk. Vele systemen die onderzoekers in België, Frankrijk en Duitsland identificeerden, werden door particuliere beveiligingsbedrijven aan de politie geleverd, vaak via concurrerende openbare aanbestedingen. Andere op data gebaseerde systemen worden intern ontwikkeld of in samenwerking met universitaire onderzoekers.

Het grootste en meest beruchte technologiebedrijf dat software voor ‘predictive’ policing in Europa verkoopt is Palantir. Drie van de 16 Duitse federale staten gebruiken momenteel systemen van dit bedrijf.²² De wereldwijde inkomsten van Palantir in 2024 bedroegen \$ 2,87 miljard.²³ Het staat internationaal bekend om de banden die het heeft met geheime diensten, legers en andere overheidsinstellingen.²⁴

Andere belangrijke bedrijven die op data gebaseerde systemen aan de politie in Europa leveren, zijn:

- Briefcam, een bedrijf uit Israël dat videotoezicht met AI vervaardigt;²⁵
- ClearView, een Amerikaans bedrijf voor gezichtsherkenning, dat vooral software levert aan strafrechtelijke autoriteiten;²⁶
- Edicia, een Frans bedrijf dat software voor ‘veiligheid in steden’ ontwikkelt;²⁷
- Simsi, een partner van de Rutgers University in New Jersey (VS) en de commerciële leverancier van het systeem Risk Terrain Modelling;²⁸
- EuroCop in Spanje, dat de afgelopen twee decennia meer dan 100 contracten afgesloten heeft met openbare diensten;²⁹



- Securitas, een Zweeds bedrijf dat ‘veiligheidsoplossingen’ aanbiedt;³⁰ en
- SopraSteria, een Frans bedrijf dat ook contracten heeft met de EU om een van de uitgebreide systemen voor biometrisch politiewerk en immigratie te ontwikkelen.³¹

Naast Briefcam hebben ook andere bedrijven uit Israël contracten met de Belgische overheid, namelijk TA9/Rayzone en Interionet. De oorsprong van TA9 is bijzonder zorgwekkend: de CEO was vroeger adjunct-directeur van Eenheid 8200, de inlichtingendienst van het Israëlische leger, die verantwoordelijk zou zijn voor de ontwikkeling van AI-systemen voor het leger.³² Heel wat ambtenaren die voor Eenheid 8200 gewerkt hebben, hebben daarna bedrijven voor privébeveiliging opgezet.³³

De technologie-industrie voor toezicht maakt momenteel een enorme groei door.³⁴ Volgens één schatting bedraagt de wereldwijde jaarlijkse groeisnelheid 12,5%. Dit betekent dat de sector in 2025 naar verwachting 186 miljard dollar waard zal zijn.³⁵ Gezien hoe winstgevend de sector duidelijk is, kunnen we verwachten dat het aantal ‘voorspellende’ systemen en de bedrijven die dit leveren in de komende jaren verder zal toenemen.



De Verordening Artificiële intelligentie van de EU

De Verordening Artificiële intelligentie van de EU is een wereldwijd baanbrekend juridisch kader voor de regulering van artificiële intelligentie, gebaseerd op de potentiële risico's voor de gezondheid, veiligheid en grondrechten. De verordening

werd in juni 2024 goedgekeurd na langdurige en complexe onderhandelingen in het Europees Parlement. De eerste elementen van de wetgeving zijn in februari 2025 in werking getreden.

De Verordening AI bevat een aantal ‘verboden AI-praktijken’, waaronder:

- ‘predictive policing’;
- biometrische identificatie op afstand (zoals gezichtsherkenning in de openbare ruimte);
- “social scoring”; en
- emotieherkenning.³⁶

Het verbod in de Verordening AI op systemen om criminaliteit te ‘voorspellen’ is vaag en onduidelijk en bevat een grote uitzondering die de impact aanzienlijk zal beperken. Het is mogelijk dat vele, zo niet alle systemen die in dit rapport en het onderliggende onderzoek³⁷ worden behandeld, niet onder het verbod van de verordening zullen vallen. Wat systemen voor predictive policing betreft, verbiedt de verordening:

“...het in de handel brengen, het voor dit specifieke doel in gebruik stellen of het gebruiken van een AI-systeem voor risicobeoordelingen van natuurlijke personen om het risico dat een natuurlijke persoon een strafbaar feit pleegt te beoordelen of te voorspellen, uitsluitend op basis van de profilering van een natuurlijke persoon of op basis van de beoordeling van zijn/haar persoonlijkheidseigenschappen en -kenmerken;

Dit wordt echter gevolgd door:

“...dit verbod geldt niet voor AI-systemen die worden gebruikt ter ondersteuning van de menselijke beoordeling van de betrokkenheid van een persoon bij een criminele activiteit, die reeds op rechtstreeks met de criminele activiteit verband houdende objectieve en verifieerbare feiten is gebaseerd.”³⁸

De wet lijkt sommige AI-systemen te verbieden die voorspellingen doen over individuen op basis van “profilering... persoonlijkheidseigenschappen en -kenmerken.” Dit is echter niet van toepassing voor AI-systemen ter “ondersteuning” van menselijke beoordeling. Deze late toevoeging aan de tekst maakt het verbod zinloos. Wetshandhaving kan eenvoudig zeggen, zoals ze reeds doen, dat ze AI gebruiken ter “ondersteuning” van menselijke beoordeling.

De tekst verwijst verder niet duidelijk naar op locatie gebaseerde of geografische systemen om misdaden te voorspellen waarvan in heel Europa ruim gebruik wordt gemaakt en verbiedt ze niet. De richtlijnen van de Europese Commissie over verboden AI-praktijken maken duidelijk dat ze niet onder de verboden praktijken vallen.³⁹ De richtlijnen zijn echter niet bindend. Als er juridische procedures worden aangespannen tegen dit soort systemen, heeft het

Hof van Justitie van de Europese Unie (HvJ-EU) waarschijnlijk uiteindelijk het laatste woord.

Het verbod wordt als “gedeeltelijk” omschreven en is aanzienlijk zwakker dan de originele versie waarover het Europese Parlement in juni 2023 gestemd heeft.⁴⁰ De overheden van de EU en de grote technologiebedrijven hebben hard gewerkt om ervoor te zorgen dat de waarborgen in de verordening afgezwakt werden.⁴¹

De Verordening AI bevat een aantal eenvoudige maatregelen voor transparantie. De verordening bepaalt dat in bepaalde gevallen, wanneer systemen als ‘hoog risico’ worden geclassificeerd, mensen geïnformeerd moeten worden over het feit dat er een AI-systeem wordt gebruikt.⁴² Als een individu het onderwerp is van een beslissing die gebaseerd is op de output van een AI-systeem dat een hoog risico inhoudt en die juridische gevolgen heeft, of die die persoon op een manier raakt die hij of zij als nadelig ervaart voor zijn of haar gezondheid, veiligheid of grondrechten, dan heeft die persoon recht op een “duidelijke en betekenisvolle uitleg” over de rol van het AI-systeem in die beslissing.⁴³

Er is echter een aanzienlijke uitzondering voorzien voor systemen die worden gebruikt om strafbare feiten op te sporen, te voorkomen, te onderzoeken en te vervolgen.⁴⁴ Als gevolg zijn er in de Verordening AI in de praktijk geen transparantieverplichtingen voor systemen voor ‘predictive’ policing of voor het ‘voorspellen’ van criminaliteit.

Daarnaast bestaat er geen zinvol mechanisme waarmee personen die de impact ondervinden van een ‘verboden AI-praktijk’ of van AI-systemen die niet aan de verordening voldoen, deze systemen kunnen aanvechten of schadevergoeding kunnen eisen voor de nadelige gevolgen van het gebruik.⁴⁵ Getroffen personen kunnen wel een klacht indienen bij een nationale autoriteit, maar de verordening legt geen verplichting op aan deze autoriteiten om daadwerkelijk een rechtsmiddel te bieden.⁴⁶

Er zijn normen vastgelegd in bestaande wetgeving inzake gegevensbescherming, meer bepaald de Algemene Verordening Gegevensbescherming (AVG) en de Richtlijn gegevensbescherming bij rechtshandhaving (LED). De laatstgenoemde is van toepassing op het gebruik van gegevens en geautomatiseerde besluitvormingssystemen door wetshandavingsinstanties. De Richtlijn gegevensbescherming bij rechtshandhaving verbiedt beslissingen die *uitsluitend* gebaseerd zijn op geautomatiseerde verwerking. Zoals hierboven vermeld, kan dit verbod echter betekenisloos blijken. Wetshandavingsinstanties kunnen eenvoudigweg beweren dat de beslissing niet uitsluitend op geautomatiseerde verwerking was gebaseerd.



Methodologie

Het onderzoek over België, Frankrijk, Duitsland en Spanje dat aan de basis ligt van dit rapport werd uitgevoerd door onderzoekers ter plaatse, met ondersteuning van de redacteurs van dit rapport.

- **Interviews:** De onderzoekers hielden interviews met experts, academici en andere onderzoekers en met ontwikkelaars van op data gebaseerde en geautomatiseerde besluitvormingssystemen. Ze spraken ook met politieambtenaren en andere functionarissen die verantwoordelijk zijn voor de werking van deze systemen. Het belangrijkste was echter dat ze mensen en groepen geïnterviewd hebben die door deze systemen en de politie en de strafrechtelijke acties waarop ze een invloed hadden getroffen worden en met mensen die met deze groepen werken.
- **Vrijheid van verzoeken om informatie:** De onderzoekers gebruikten wetgeving inzake vrijheid van verzoeken om informatie om aanvragen in te dienen bij lokale en nationale politiediensten, overheidsdiensten, gevangenis- en reclasseringsinstanties.
- **Open source-onderzoek:** De onderzoekers bestudeerden openbare documenten zoals contracten, financiële verslagen, interne evaluatierapporten en studies, effectbeoordelingen, websites en brochures van bedrijven en gerelateerde informatie.
- **Analyse van bestaande academische literatuur:** De onderzoekers bestudeerden en analyseerden studies en rapporten over deze systemen, in het bijzonder technische studies over hun ontwerp, opleiding en werking.

Problemen in verband met transparantie

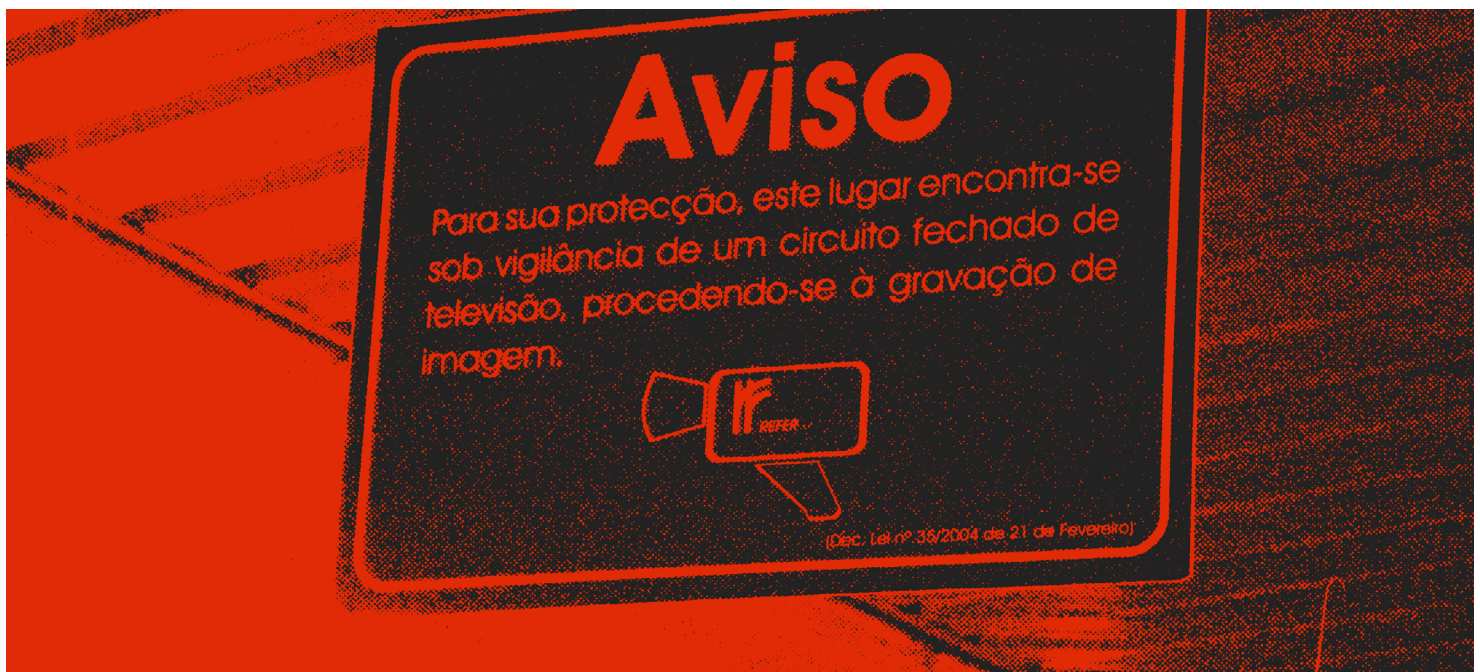
Uit het onderzoek in alle betrokken landen blijkt duidelijk dat de politie en strafrechtelijke autoriteiten proberen om de vrijgave of publicatie van informatie over ‘voorspellende’, profilerings- en risicobeoordelingssystemen te beperken of te voorkomen.

In alle landen werden formele verzoeken van onderzoekers aan overheidsdiensten, politiediensten en lokale overheden afgewezen of genegeerd, vaak op basis van bedrijfsgeheim of dreigingen voor de nationale veiligheid.⁴⁷ Wanneer overheidsdiensten wel antwoordden, was de verstrekte informatie vaak beperkt en ontwijkend.⁴⁸ Private bedrijven leveren ondertussen een aanzienlijk deel van de infrastructuur en operationele tools aan de politie. De wetgeving inzake openbaarheid van bestuur is echter niet op hen van toepassing.⁴⁹

Verzoeken om interviews werden ook vaak afgewezen of genegeerd. In Spanje deed *AlgoRace* meerdere verzoeken tot interviews bij overheidsdiensten. Die verzoeken werden afgewezen, ondanks het feit dat de betrokken personen individueel wel bereid waren om te spreken.

Het niveau van transparantie rond deze systemen is volkomen onaanvaardbaar, zeker gezien de ernstige technische, juridische en politieke kwesties die ze oproepen.





Op locatie gebaseerde ‘voorspellende’ systemen

De op locatie gebaseerde methoden voor ‘predictive policing’ werden ontwikkeld om te voorspellen waar en vaak ook wanneer een misdrijf zal plaatsvinden, zodat politiediensten hun middelen daar kunnen inzetten. De onderzoekspartners vonden voorbeelden van geografische ‘voorspellende’ algoritmen voor criminaliteit in alle onderzochte landen: België, Frankrijk, Duitsland en Spanje.

Voorstanders van op locatie gebaseerde systemen voor ‘predictive policing’ beweren dat op data gebaseerde benaderingen het politiewerk efficiënter kunnen maken. Door de locaties te identificeren die de grootste dreiging vormen, zo luidt het argument, kunnen politiediensten misdrijven voorkomen. Deze benadering wordt als volgt samengevat:

“Als de politie haar middelen kan richten op risicovolle personen, plaatsen en tijdstippen, zal ze effectiever zijn in het terugdringen van criminaliteit binnen haar rechtsgebieden”.⁵⁰

Onderzoekers hebben in Europa twee belangrijkste soorten op locatie gebaseerde systemen geïdentificeerd:

- algoritmes die ‘hotspots’ van misdaad voorspellen, waarbij historische politiegegevens gebruikt worden om plaatsen waar in de toekomst misdrijven gepleegd zullen worden te voorspellen; en
- algoritmes om risico’s te voorspellen, gebaseerd op de veronderstelling dat

omgevingsfactoren bepalen waar misdaden gepleegd worden.

Beide methoden roepen zorgwekkende vragen op over de onevenredige gerichtheid op raciaal gemarginaliseerde en financieel kwetsbare personen en gemeenschappen en de criminalisering ervan.

De voorbeelden in dit rapport tonen aan dat op locatie gebaseerde predictive policing ernstige gevolgen kan hebben voor mensen die wonen en werken in gebieden die als ‘hoog risico’ worden bestempeld. Zij kunnen geconfronteerd worden met verhoogde politiebewaking, monitoring, voertuig- en identiteitscontroles, fouilleringen, ondervragingen en zelfs arrestaties.

Hoewel de EU Verordening AI een formeel verbod bevat op bepaalde soorten ‘voorspellende’ politiestystemen, vallen op locatie gebaseerde ‘voorspellende’ systemen volgens de officiële richtlijnen niet onder dat verbod.⁵¹ Het onderzoek maakt duidelijk dat deze systemen een groot potentieel hebben voor discriminatie en profilering. Ze moeten daarom worden opgenomen in elk betekenisvol verbod op predictive policing.

Dit rapport biedt slechts een momentopname van de geografische systemen om misdaad te ‘voorspellen’ die de politiediensten in Europa gebruiken. Naast de systemen in Frankrijk, België, Duitsland en Spanje zijn er ook soortgelijke voorbeelden in Italië, Zwitserland en het Verenigd Koninkrijk, zoals eerder onderzoek heeft aangetoond.

Voorspelling van ‘hotspots’ voor criminaliteit

Op locatie gebaseerde systemen in België, Frankrijk, Duitsland en Spanje maken voornamelijk gebruik van methoden om ‘hotspots’ voor misdaad te voorspellen. Daarbij worden historische misdaadcijfers, die aangeven waar en wanneer misdrijven plaatsvonden, gebruikt om de locaties van toekomstige misdaden (‘hotspots’) te voorspellen.

Onderzoekers hebben ten minste negen verschillende systemen geïdentificeerd om ‘hotspots’ te voorspellen. Veel van deze systemen worden uitgerold door meerdere politiediensten in elk land.

In Duitsland:

- De politie van Berlijn rolt een strategie uit om *kriminalitätsbelastete Orte* (kbO's) ofwel ‘misdadigevoelige plaatsen’ in te delen, waar de politie ruimere bevoegdheden kan gebruiken;⁵²
- Drie Duitse federale staten gebruiken ‘hotspots’-systemen voor misdaad, in vergelijking met zes staten die vijf verschillende systemen gebruikten in 2018.⁵³ Deze systemen zijn:
 - SKALA (*System zur Kriminalitätsauswertung und Lageantizipation*, Systeem voor de analyse van misdaad en anticipatie van situaties) in Noordrijn-

Westfalen;

- KrimPro (*Kriminalitätsprognose Wohnraumeinbruch*, Voorspelling van criminaliteit voor inbraak in privéwoningen) in Berlijn; en
- KLB-operativ (*Kriminalitätsslagebild*, Bewustzijn van misdaadsituaties) in Hesse;⁵⁴ and en
- De politie in Beieren heeft het re-Crime Observation System (PRECOBS) gebruikt.⁵⁵

In Spanje worden op locatie gebaseerde ‘voorspellende’ systemen ruim gebruikt:

- Het ‘Predictive Police Patrolling Decision Support System (P3-DSS) wordt op het hele grondgebied gebruikt;⁵⁶ en
- Zeven regio’s gebruiken een systeem van EuroCop, inclusief bijna alle politiediensten in Madrid.⁵⁷

In Frankrijk en België hebben onderzoekers minder actieve voorbeelden van politiemethodes via ‘hotspots’ gevonden. In Frankrijk heeft *La Quadrature du Net* ‘PredVol’ en PAVED aangetroffen. Beide systemen werden door de *Gendarmerie Nationale* gebruikt maar dit is nu niet meer het geval.⁵⁸

In België heeft *TechnoPolice* een kleine test gevonden bij de politie van de Westkust en het gebruik van het Geographic Information System, gemaakt door Orbit, in Vlaanderen en Brussel.⁵⁹ Orbit beweert dat de software van het bedrijf “al in bijna 100 politiezones gebruikt wordt”.⁶⁰

Systemen om ‘hotspots’ voor criminaliteit te voorspellen, hebben internationaal veel kritiek gekregen nadat een onderzoek gevoerd werd naar het PredPol-systeem in de VS omdat het raciale vooroordelen zou versterken en in stand houden.⁶¹

De systemen die in dit rapport worden besproken, waarvan sommige vergelijkbare methoden gebruiken als PredPol, roepen eveneens serieuze vragen op over discriminatie en criminalisering. In alle vier onderzochte landen zijn de gebieden die door ‘hotspots’-systemen voor misdaad als ‘hoog risico’ worden bestempeld vaak de buurten waar gemarginaliseerde gemeenschappen wonen en werken.

Doelen

De politie beweert dat ze met statistische berekeningen om ‘hotspots’ voor criminaliteit te voorspellen de criminaliteitscijfers kunnen verlagen. Florian Gauthier, de Franse dataspecialist

die PredVol ontwikkelde, rechtvaardigt de noodzaak van politiewerk op ‘hotspots’ om autodiefstallen te voorspellen door te wijzen op de discrepanties tussen de plekken waar agenten patrouilleren en de locaties waar autodiefstallen daadwerkelijk plaatsvinden. Deze discrepanties, zo suggereert hij, kunnen worden verminderd door politiediensten te sturen op basis van misdaadcijfers.⁶²

Met deze zogenaamde ‘op bewijs gebaseerde’ methoden zouden agenten op het juiste moment naar de juiste plaats kunnen worden sturen, zodat criminele activiteiten kunnen worden ontmoedigd nog vóór ze plaatsvinden. In Duitsland beweert de politie van Berlijn dat het aanduiden van een gebied als een kbO (Kriminalitätsbelasteter Ort) het “veiligheidsgevoel” vergroot, omdat de politie er “de identiteit van relevante personen kan controleren, de kans om betrapt te worden kan verhogen en zo strafbare feiten kan voorkomen”.⁶³

Vele van de geïdentificeerde voor ‘hotspots’-systemen zijn voor zogenaamde diefstallen of inbraken:

- in Frankrijk dient PredVol zogenaamd voor autodiefstallen en PAVED⁶⁴ voor autodiefstallen en inbraken;
- In Duitsland focust het PRECOBS-systeem zogenaamd op autodiefstallen en inbraken, terwijl het systeem van de KbO zich concentreert op diefstal, naast andere misdrijven;⁶⁵ Onderzoekers hebben geopperd dat de ‘hotspots’-systemen voor inbraken ingevoerd werden in de jaren 2010-2020 als een respons op paniek in de media over inbraken.⁶⁶
- In België focust het ‘voorspellende’ systeem van de lokale politie van de Westkust zich op inbraken en autodiefstallen,⁶⁷ en
- in Spanje probeert het EuroCop-systeem diefstallen en andere misdrijven te ‘voorspellen’;⁶⁸

Gebruikte data

Systemen voor de voorspelling van ‘hotspots’ voor criminaliteit halen statistische inzichten en trends uit grote hoeveelheden criminaliteitsgegevens, vaak afkomstig uit politiedatabanken, om te voorspellen waar toekomstige misdrijven zullen plaatsvinden.

In Duitsland gebruikt het op locatie gebaseerde model om criminaliteit te voorspellen, bekend als kbO (Kriminalitätsbelastete Orte, plekken met een hoge criminaliteitsdruk), een statistische beoordeling op basis van misdaadcijfers en andere niet-gespecificeerde aanvullende informatie.⁶⁹

In België gebruikt het Orbit Geographic Information System, dat blijkbaar door meer dan 100 lokale politiediensten gebruikt wordt, politieverslagen over misdaad uit het verleden om toekomstige ‘hotspots’ voor criminaliteit te identificeren.⁷⁰ De lokale

politiediensten van de Westkust gebruiken ook politiegegevens over zogenaamde misdrijven, nummerplaten, verslagen van de rechtbank en zelfs het weer.⁷¹

In Frankrijk gebruikt PredVol data over autodiefstallen uit de IT-systemen die gebruikt worden om alle klachten en verslagen bij te houden, met inbegrip van:

- xy-coördinaten waar de autodiefstallen plaatsvonden;
- datum; en
- extra informatie over het model van het voertuig en de kleur.⁷²

In Spanje gebruikt EuroCop allerlei bronnen van informatie, zoals gegevens en bestanden van de politie in verband met misdaad, socio-economische gegevens en gegevens afkomstig van videotoezicht. Dit alles wordt gebundeld in een algoritmisch model om misdaad te ‘voorspellen’ en om ‘heatmaps’ en ‘patrouilletrajecten’ voor de politie te creëren.⁷³

Er is ernstige bezorgdheid dat historische politiedata in ‘hotspots’-systemen voor criminaliteit zullen leiden tot onwettige discriminatie. Zoals later zal worden toegelicht, weerspiegelen historische misdaadcijfers overmatig politiewerk en criminalisering van geracialiseerde en kansarme gemeenschappen. ‘Hotspots’-algoritmes voor criminaliteit dragen deze ongelijkheid en discriminatie over naar toekomstige voorspellingen.



De Belgische minister van Binnenlandse Zaken erkende dit in juni 2020 expliciet: “Politiestatistieken zijn in de eerste plaats een weerspiegeling van de politieactiviteit. Ze geven niet de realiteit van de criminaliteit in een bepaald gebied weer.”⁷⁴

Veel ‘hotspots’-systemen maken in hun trainingsdatasets ook gebruik van sociaal-demografische gegevens. De ontwikkelaar van PredVol vertelde aan *La Quadrature du Net* dat het systeem 600 sociaal-demografische variabelen gebruikt. Deze omvatten aanwezigheid op school en werkloosheidsgraad, het aantal nabijgelegen winkels en de gemiddelde leeftijd van de bevolking. De autoriteiten weigerden uitgebreidere informatie te verstrekken.⁷⁵ Ook bleek dat PAVED, van de 15 gebruikte sociaal-demografische variabelen, onder

meer gegevens inzette over geslacht, nationaliteit en migratiestatus, gezinsinkomen en opleidingsniveau.⁷⁶

Het ‘Smart Patrolling’-systeem P3DSS van de Spaanse nationale politie maakte eveneens gebruik van nationaliteitsgegevens, waarbij de inwoners van Madrid in groepen ingedeeld worden: Spaanse staatsburgers, andere EU-burgers, niet-EU-burgers, en opmerkelijk genoeg ook burgers per continent.⁷⁷ Het systeem berekende vervolgens voor elke nationaliteitsgroep een “doel voor politiecontact”: de hoeveelheid patrouilletijd die aan elke groep moest worden toegewezen op basis van haar omvang in verhouding tot het geografische gebied.⁷⁸ Deze demografische groepen fungeren in wezen als tijdelijke vervangers voor raciale categorieën, hoewel ze erg algemeen zijn.

Gegevens over nationaliteit, immigratiestatus en gender zijn allemaal (of kunnen beschouwd worden als) “speciale categorieën” van data.⁷⁹ Deze en andere sociaal-demografische variabelen houden een risico in dat er correlaties gelegd worden tussen criminaliteit en ras of economische achterstand. De Europese wet inzake gegevensbescherming stelt dat:

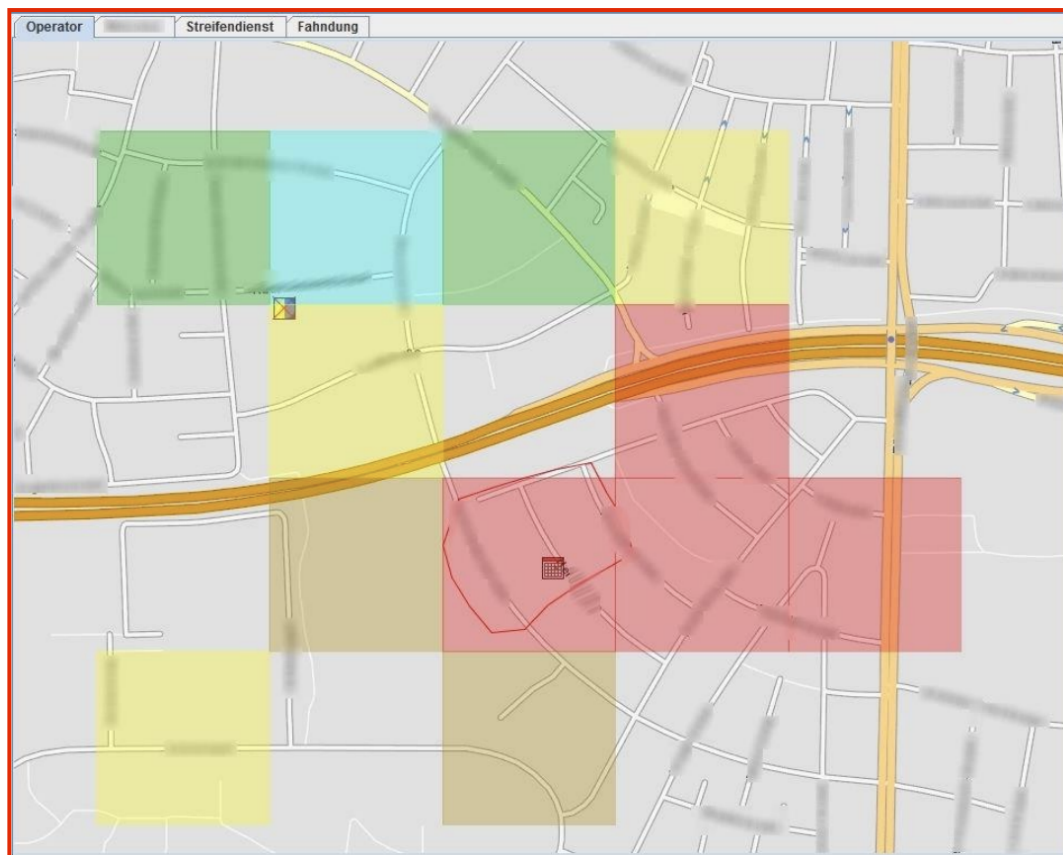
“Profilering die leidt tot discriminatie van natuurlijke personen op grond van persoonsgegevens die door de aard ervan bijzonder gevoelig zijn wat betreft de grondrechten en fundamentele vrijheden, dient verboden te worden.”⁸⁰

Op basis van deze inputgegevens gebruiken ‘hotspots’-systemen statistische analyses om de waarschijnlijkheid van toekomstige criminaliteit op specifieke locaties te voorspellen. De specifieke modelleertechnieken voor deze geografische en temporele analyses verschillen per systeem.

PAVED en PredVol gebruiken machinaal lerende technieken, wat betekent dat de systemen automatisch ‘leren’ van extra gegevens, zonder dat ze handmatig opnieuw getraind hoeven te worden. De meeste andere ‘hotspots’-systemen die zijn geïdentificeerd in België, Frankrijk, Duitsland en Spanje gebruiken algoritmische methoden.

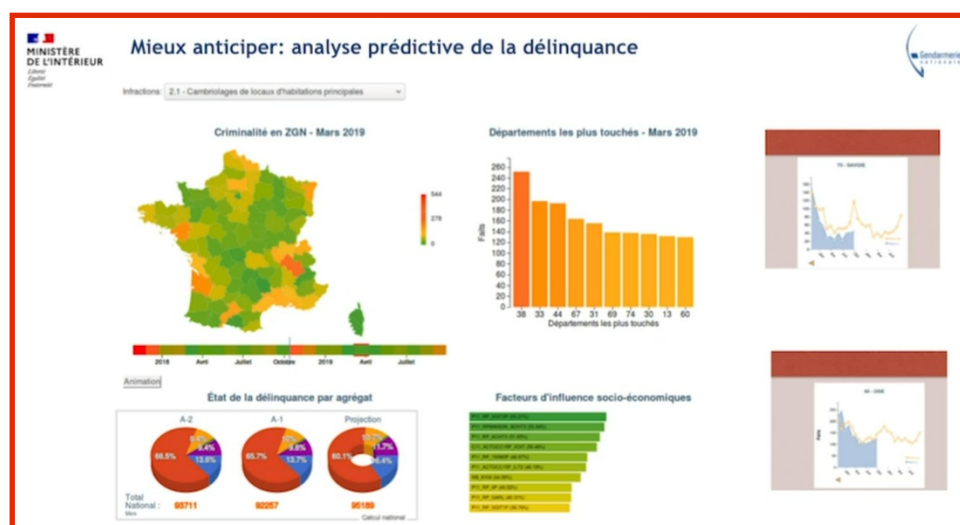
Resultaten

In het algemeen geven deze systemen om ‘hotspots’ te voorspellen de politie een heatmap om gebieden of locaties te voorspellen waar er een hoog risico op misdaad zou zijn. Zo toont PRECOBS in Duitsland een kaart met gebieden die in verschillende kleuren zijn aangeduid. Deze kleuren vertegenwoordigen de veronderstelde waarschijnlijkheid, of risiconiveaus, dat er in dat gebied een misdrijf zal plaatsvinden (zie figuur 1).



FIGUUR 1: EEN SCREENSHOT VAN DE KAART VAN PRECOBS VAN EEN LOCATIE MET KLEURCODES.
BRON: SONJA PETERANDERL

Sommige systemen, zoals PredVol in Frankrijk, kunnen door agenten ‘op het terrein’ gebruikt worden met tablets. Andere systemen, zoals PAVED, zijn alleen toegankelijk voor leidinggevenden. Naast ‘heatmaps’ toont PAVED ook histogrammen met de sociaal-demografische variabelen die als de meest invloedrijke indicatoren voor criminaliteit worden beschouwd (zie figuur 2).



FIGUUR 2: SCREENSHOT VAN DE LEZING VAN KOLONEL PATRICK PERROT, COLLOQUE DE L'INSTITUT DE DROIT PRIVÉ—UT CAPITOLE—SEPTEMBER 8, 2021 (BRON: “AI ET ENJEUX DE SÉCURITÉ,” OP 23M10S).

Deze systemen om ‘hotspots’ voor criminaliteit te voorspellen worden gebruikt om de middelen van de politie toe te wijzen en te bepalen waar en wanneer politieagenten patrouilles uitvoeren. Gevolgen in ‘hotspots’ zijn bijvoorbeeld:

- toezicht;
- informatievergaring;
- identiteitscontroles;
- ondervragingen;
- fouilleren;
- straatverbod; of
- arrestaties.⁸¹

De aanduiding van gebieden als ‘hotspots’ kan ook leiden tot verruimde politiebevoegdheden in die locaties. In Berlijn is de politie wettelijk gemachtigd om identiteitscontroles of fouilleringen van personen of objecten uit te voeren in zogenaamde ‘kbO’s’ zonder concrete verdenking, maar op basis van “gedrag”.⁸²

In een vergelijkbare situatie sprak *La Quadrature du Net* met een bron die uitlegde dat ‘hotspots’ die gegenereerd werden door PAVED werden gebruikt om aanklagers/ procureurs te overtuigen om speciale bevelen uit te vaardigen voor identiteits- en voertuigcontroles in die gebieden. Door deze machtigingen kon de bestuurlijke politie gerechtelijke politietaken uitvoeren. Dit is een ernstige schending van de bevoegdheden van de bestuurlijke politie.⁸³



Impact

Locaties die door algoritmische systemen worden aangeduid als ‘hotspots’ voor criminaliteit zijn onevenredig vaak wijken of buurten waar mensen met een laag inkomen en geracialiseerde gemeenschappen wonen en werken. Juridische experte Lina Schmid merkt op dat plaatsen die als ‘kbO’s’ worden aangemerkt, doorgaans plekken zijn waar zich een hoog percentage mensen bevinden die als migranten worden gezien.⁸⁴

Na de invoering van het PRECOBS-systeem in Beieren stelde Matthias Monroy, de uitgever van het Duitse tijdschrift voor burgerrechten *Bürgerrechte & Polizei* (*Burgerrechten en politiewerk*) dat:

“Wie wordt er vaker tegengehouden door de politie wanneer ze denken dat er in de komende uren of dagen een inbraak zal plaatsvinden? Ik zou zeggen dat het meer waarschijnlijk is dat het mensen zijn in versleten kleren, mensen met een andere huidskleuren of met hoodies; patronen die al bestaan binnen de politie.”⁸⁵

In Duitsland zijn controles die de politie uitvoert op basis van raciale toekenning verboden door de grondwet (Artikel 3 van de *Grundgesetz* [Grondwet]). Lina Schmid legt uit dat de politie dit verbod echter omzeilt door bepaalde gebieden als ‘hotspots’ voor criminaliteit aan te duiden:

“Hier worden in plaats van geracialiseerde groepen mensen, zoals gebruikelijk is bij etnisch profileren, volledige plekken en de mensen die zich daar bevinden gecriminaliseerd. Dit creëert ruimte voor de politie om op een verborgen manier aan etnisch profileren te doen, omdat, zelfs als zogenaamd alle mensen worden gecontroleerd, het in de praktijk nog steeds vooral BIPOC [Black, Indigenous and People of Colour] [zwarte mensen, inheemse mensen of mensen van kleur] zijn die de politie viseert.”⁸⁶

Het bewonersinitiatief *Wrangelkiez United* vertelde dat controles in het Görlitzer Park/ Wrangelkiez kbO bijna uitsluitend uitgevoerd worden op zwarte mensen en raciaal als minderheid behandelde mensen, “ongeacht wat ze aan het doen zijn of waar ze naartoe gaan.”⁸⁷ De studenten van een talenschool in de buurt worden gecontroleerd op weg naar school en zwarte mannen worden regelmatig in het park gecontroleerd, zoals gerapporteerd in de video-interviews met *Wrangelkiez United*:

“Wanneer de politie aanwezig is (...) dan is de kans groter dat mensen met een donkere huidskleur zoals ik zonder geldige reden gecontroleerd worden. We hebben geen misdaden gepleegd. Het is vanwege ons uiterlijk.”⁸⁸

Voorspelling van ‘risico’

Op locatie gebaseerde systemen in Europa omvatten ook systemen om ‘risico’s’ te voorspellen die omgevings- of contextuele data gebruiken om locaties te identificeren die zogenaamd vatbaarder zouden zijn voor criminaliteit.

Deze op omgeving gebaseerde systemen om ‘risico’s’ te voorspellen zijn gebaseerd op de criminologische ‘Broken Windows Theory’. Deze theorie stelt dat de fysieke omgeving een bepalende factor is voor criminaliteit. Ze werd in 1982 in de VS geïntroduceerd door James Wilson en George Kelling.⁸⁹ De theorie gaat uit van veronderstellingen waarbij omgevingsfactoren (zoals kapotte ramen) worden gezien als indicatoren of juist als afschrikmiddelen voor crimineel gedrag.

Politiewerk op basis van “gebroken ramen” werd vervolgens ingevoerd binnen de Amerikaanse politiediensten. Een vaak aangehaald voorbeeld zijn de veranderingen die de voormalige politiecommissaris van het New York Police Department, William Bratton invoerde.⁹⁰ Dit ontpopte zich tot de basis van de op data gebaseerde politiemethodes, hoewel het voor het grootste deel ontkracht werd door criminologen en sociologen.⁹¹

Net als bij ‘hotspots’-algoritme, voor criminaliteit kunnen op omgeving gebaseerde ‘risico’-algoritmen de politie naar stadsgebieden leiden die economisch achtergesteld zijn, en die vaker bewoond en bezocht worden door geracialiseerde gemeenschappen.

Doelen

De Belgische en Franse politie gebruiken een algoritmisch model dat ‘Risk Terrain Modelling’ genoemd wordt om misdaad of criminaliteit te voorspellen. Dit houdt een beoordeling van het ‘risico’ van de omgeving in. Ook de politie in het VK gebruikt dit.⁹²

De methodologie “Risk Terrain Modelling (RTM)” werd ontwikkeld door Joel Caplan en Leslie Kennedy, twee academici aan de Rutgers University in New Jersey in de VS. Deze methode zou getest zijn in meer dan 45 landen op zes continenten. De website van Risk Terrain Modelling, die de software promoot die het bedrijf Simsi ontwikkelde, stelt:

“Wat risk terrain modeling (RTM) doet, is de risico’s identificeren die voortkomen uit kenmerken van een landschap, en modelleren hoe deze samenkomen om unieke gedragsomgevingen voor criminaliteit te creëren.

Je kunt je waarschijnlijk het clichébeeld van een ‘donkere steeg’ voorstellen als je denkt aan potentiële locaties voor criminele activiteiten. In dit geval neem je minstens twee kenmerken van een landschap in overweging: (1) een steeg en (2) slechte verlichting. Er wordt aangenomen dat het risico op criminaliteit uitzonderlijk

*hoog is op plaatsen waar deze specifieke kenmerken samen voorkomen.*⁹³

De website maakt een onderscheid tussen Risk Terrain Modelling en methodes om ‘hotspots’ voor criminaliteit te voorspellen:

*“Hotspots vertellen waar er clusters van misdaad zijn, maar niet noodzakelijk waarom. Mensen concentreren zich te vaak op hotspots zonder ook evenveel aandacht te besteden aan de ruimtelijke kenmerken die ervoor zorgen dat die plaatsen dat worden.... Hotspots zijn enkel tekenen en symptomen van plaatsen die erg geschikt zijn voor misdaad. RTM doet dit door een diagnose over de ruimte te geven.”*⁹⁴

Risk Terrain Modelling wordt momenteel gebruikt in de Zennevallei (België) en Parijs (Frankrijk). De *Direction de la Sécurité de Proximité de l’Agglomération Parisienne* (DSPAP, Directie voor lokale veiligheid van de agglomeratie van Parijs) begon het algoritme te gebruiken nadat een geo-statisticus bij het voormalige *Observatoire National de la Délinquance et des Réponses Pénales* (ONDRP, of Nationaal observatorium voor criminaliteit en strafrechtelijke respons)⁹⁵ enkele jaren met de Rutgers University samengewerkt had. Hij stelde:

*“Ik gebruik het RTM-algoritme (Risk Terrain Modelling) al meer dan acht jaar... Het is nu een webapplicatie, veel krachtiger dan ze vroeger was, maar het gebruikt nog altijd hetzelfde principe: het ligt in mijn met situationele criminaliteitspreventie. Dit betekent dat we de contextuele en omgevingsfactoren identificeren die misdaad mogelijk maken. Dus door een omgeving te analyseren en de factoren te identificeren die het risico verergeren, kunnen we voorspellen wat er in een vergelijkbare omgeving zou kunnen gebeuren.”*⁹⁶

In de Zennevallei wordt het voor gelijkaardige doelen gebruikt. Daar werd het programma geleid door Anneleen Rummens, doctoraatsstudente aan de Universiteit van Gent, onder supervisie van professor in de criminologie Wim Hardyns.⁹⁷

Er zijn andere systemen die het ‘omgevingsrisico’ voorspellen en die het algoritme van Risk Terrain Modelling niet gebruiken. Dit zijn bijvoorbeeld MapRevelation en de ‘voorspellende module’ van het Smart Police-systeem in Frankrijk. MapRevelation was een van de eerste ‘voorspellende’ systemen voor politiewerk dat in Frankrijk ingevoerd werd. Het wordt op de markt gebracht door het bedrijf Sûreté Globale⁹⁸ en wordt gebruikt door lokale overheden en de gemeentelijke politiediensten in Montpellier, Lyon, Rijsel, Villeurbanne, Montauban, Angers, Colombes en Melun Val de Seine.⁹⁹

Gebruikte data

Het Risk Terrain Modelling-systeem gebruikt verschillende wegingsfactoren die in het eindmodel ingevoerd worden. Deze factoren kunnen aangepast worden afhankelijk van het specifieke gebruik van het model. Het algoritme kent een bepaalde gevoeligheidswaarde toe aan locaties op basis van ruimtelijke factoren zoals:

- of de locatie goed verlicht is;
- metro- en busstations;
- ruimtes om buiten te zitten of cafés;
- fastfoodrestaurants;
- openbare toiletten;
- apotheken;
- winkels;
- bars;
- bomen en banken;
- bepaalde soorten winkels;
- scholen;
- postkantoren;

Op de website van Risk Terrain Modelling worden er nog andere factoren aangehaald, zoals ‘drugs’, ‘leegstand’, en ‘bendes’.¹⁰⁰

In Parijs gebruikt het Risk Terrain Modelling-systeem data van de LRPPN, de *Logiciel de Rédaction des Procédures de la Police Nationale* [Software om procedures voor de nationale politie op te stellen]. Het leidt correlaties af tussen misdaden en zogenaamde omgevingsfactoren. In 2018 gaf Jean-Luc Besson, het hoofd van de geostatistische afdeling van ONDRP, een inzicht in welke factoren in het Parijse model gebruikt kunnen worden:

“Als we kijken naar gauwdieven bij geldautomaten, stellen we ons de vraag: zijn de meest getroffen geldautomaten dag en nacht open? Bevinden ze zich op een kruispunt of in een treinstation, enzovoort?”¹⁰¹

De onderzoekers konden geen precieze informatie verkrijgen over alle variabelen die



in Parijs en de Zennevallei gebruikt worden in de Risk Terrain Modelling-systemen. Het is echter wel bekend dat het model van de Zennevallei factoren zoals weersomstandigheden bij bepaalde gebeurtenissen gebruikt.¹⁰²

In Frankrijk zou MapRevelation getraind zijn op een ‘terrorismedatabank’ om aanvallen te ‘voorspellen’.¹⁰³ Het wordt ook gevoed door data van de gemeentelijke politiediensten die het systeem gebruiken.

De ‘voorspellende module’ van Smart Police, die door het Franse bedrijf Edicia gebruikt werd, gebruikt machinaal lerende technieken. Het gebruikt operationele politiegegevens (bijvoorbeeld verslagen, inbreuken, locatie van agenten en voertuig) en gegevens over de stad (bijvoorbeeld over de omgeving en het weer, nationale en plaatselijke evenementen, sociaal-demografische en electorale gegevens).

De ‘voorspellende’ module van Smart Police zou ook informatie halen uit de sociale media en bij andere partners. Dit omvat ook directeurs van middelbare scholen en eigenaars van sociale woningen, naast directe kennis van politieagenten.¹⁰⁴ Dit houdt uiteraard een risico in dat geruchten, roddels en niet-gecontroleerde opinies in de algoritmische systemen opgenomen worden, onder de vermomming van technische objectiviteit.

Resultaten

Een cultuur van geheimhouding binnen politiediensten en overheidsinstanties maakte het moeilijk om sluitende informatie te vinden over de resultaten van de op omgeving gebaseerde systemen om ‘risico’ te voorspellen die in België en Frankrijk worden gebruikt.

Volgens een bron die werd gecontacteerd door *La Quadrature du Net* is er geen sluitend bewijs dat het Risk Terrain Modelling-systeem in Frankrijk leidt tot een vermindering van de criminaliteitscijfers. De bron gaf ook aan dat door de Risk Terrain Modelling-methodologie instellingen mogelijk reflectie over de structurele oorzaken van criminaliteit vermijden.¹⁰⁵ Een soortgelijk probleem doet zich voor bij andere systemen voor de voorspelling van ‘hotspots’ voor criminaliteit.

Andere op locatie gebaseerde systemen om criminaliteit te ‘voorspellen’ die in Europa worden gebruikt

Naast de hierboven beschreven systemen in België, Frankrijk, Duitsland en Spanje gebruiken ook andere politiediensten in Europa op locatie gebaseerde predictive policing-systemen.

In het VK ontdekte *Amnesty International UK* onlangs dat bijna drie vierde van de politiediensten ‘predictive policing-systemen gebruikt, waarbij 32 van de 46

politiediensten op locatie gebaseerde systemen inzetten om criminaliteit te ‘voorspellen’.¹⁰⁶ Amnesty onderzocht het gebruik van Risk Terrain Modelling door Britse politiediensten en concludeerde dat het gebruik van deze methode door de Metropolitan Police in Londen “bijdraagt aan raciale profilering en discriminerend politiewerk en dit nog versterkt”.¹⁰⁷ Demografische analyses van de gebieden die door het Risk Terrain Modelling-algoritme als ‘hoog risico’ werden bestempeld, toonden aan dat:

“...de gebieden waar het Risk Terrain Modelling-systeem ernstige gewelddadige criminaliteit voorspelde, in hoge mate overeenkwamen met gebieden met een grotere populatie van kansarme bewoners van Afrikaanse, Caribische, Bengaalse en Pakistaanse afkomst.”¹⁰⁸

Reflecterend op het gebruik van op omgeving gebaseerde ‘risicofactoren’ voor het ‘voorspellen’ van criminaliteit, zei Dr. Adam Elliott-Cooper, academicus en auteur van *Black Resistance to British Policing*:

“[W]e zouden niet verbaasd moeten zijn dat het soort bebouwde omgeving dat de politie viseert, niet de halfopen woningen met een wit tuinhekje zijn. Het zullen sociale woonwijken zijn, stedelijke binnenstadsgebieden waar de politie nu al erg aanwezig is, niet de welvarende buitenwijken. We zien dus hoe deze zogenaamd geografische en daarmee zogenaamd meer wetenschappelijke en objectieve benadering van politiewerk in werkelijkheid gewoon bestaande problemen reproduceert.”¹⁰⁹

In Nederland gebruikt de politie het ‘Criminaliteits Anticipatie Systeem’ (CAS). Dit systeem om ‘hotspots’ te voorspellen baseerde zich oorspronkelijk op data zoals het aantal ‘niet-Westerse’ personen met ten minste één in het buitenland geboren ouder in een bepaald gebied. Hoewel deze datapunten later werden verwijderd, bleef het systeem historische misdaadcijfers en indirecte indicatoren voor ras en sociale klasse gebruiken, zoals gegevens over inkomens en uitkeringen.¹¹⁰

De Italiaanse politie gebruikte voordien ‘Delia’, een systeem dat door het bedrijf KeyCrime ontwikkeld werd. Dit heeft zowel geografische als individuele functies om criminaliteit te ‘voorspellen’. Het zou een van de eerste voorbeelden in de wereld zijn van commercieel beschikbare software voor predictive policing, die al in 2008 operationeel was.¹¹¹ KeyCrime is echter in liquidatie gegaan door de financiële onzekerheid die gepaard ging met de invoering van de Europese Verordening inzake AI en de mogelijkheid dat het systeem in de toekomst verboden zou kunnen worden.¹¹²

Er wordt nu een systeem, XLAW, gebruikt in Italië.¹¹³ XLAW is een op omgeving gebaseerd systeem om risico te voorspellen, dat vergeleken kan worden met de Risk Terrain Modelling-systemen die in Frankrijk, België en het VK gebruikt worden. De ruimtelijke

en tijdelijke voorspellende factoren van het systeem omvatten: grote plaatsen, pensioenen betaald aan het einde van de maand, de sluitingsuren van winkels, aankomst van treinen en boten en schommelingen in het weer.¹¹⁴

In sommige kantons in Zwitserland gebruikt de politie PRECOBS, het systeem dat ook in Duitsland gebruikt wordt.¹¹⁵





Op individuen gerichte systemen om criminaliteit te ‘voorspellen’ en te profileren

Op personen gerichte tools om criminaliteit te ‘voorspellen’ zijn bedoeld om te voorspellen hoe waarschijnlijk het is of welk risico er bestaat dat deze persoon bepaalde daden zou uitvoeren, vooral daden die als misdaden beschouwd worden. In plaats van zich te concentreren op een bepaalde locatie, focussen ze op bepaalde individuen.

De politie en strafrechtelijke autoriteiten gebruiken deze systemen om het ‘risico’ dat een persoon een misdaad pleegt of gecriminaliseerd gedrag vertoont te ‘voorspellen’ of beoordelen en deze persoon te profileren. Andere gelijkaardige systemen proberen in te schatten hoe groot de kans is dat iemand het slachtoffer van een misdaad wordt, zoals gendergebaseerd geweld. Ze worden ook gebruikt om te proberen om zogenaamde valse meldingen van misdaden op te sporen.

De gegevens van de mensen waarop deze systemen gericht zijn, worden geanalyseerd: hun leven in het verleden en het heden en hun relaties. Het doel is om hun gedrag, het ‘risico’ dat ze inhouden of hun veronderstelde ‘criminaliteit’ te bepalen en ‘voorspellen’.

Dit kan eventueel ernstige gevolgen hebben. Deze systemen kunnen ervoor zorgen dat mensen onder toezicht of monitoring geplaatst worden. Ze kunnen geconfronteerd worden met een toename in politiecontroles, ondervragingen, fouilleringen, bezoeken aan huis of op het werk. Het gebruik van deze systemen kan zelfs leiden tot detentie, arrestatie of deportatie.

Deze systemen worden ook gebruikt in het strafrechtelijke systeem. Ze kunnen een impact hebben op de beslissingen van rechters, bijvoorbeeld op veroordelingen. Dit kan een invloed hebben op de lengte van de gevangenisstraf, wanneer de persoon vrijkomt en de omstandigheden waarin ze aangehouden blijven.

Doel

Op personen gerichte ‘voorspellende’ systemen en systemen voor profilering en het beoordelen van ‘risico’ worden gebruikt voor een brede waaier doelen. Sommige politiediensten gebruiken datamining- en analysesoftware om data te verzamelen en te combineren, patronen te analyseren, en die te gebruiken om toekomstige patronen te ‘voorspellen’.

In Duitsland beschikken drie deelstaten over licenties voor programma’s voor ‘big data mining’ en analyse, gebaseerd op de Gotham-software van het Amerikaanse technologiebedrijf Palantir. Net zoals veel andere bedrijven die politietechnologie ontwikkelen en verkopen, doet Palantir uiterst geheimzinnig over zowel de technologie als de contracten die het afsluit.

De politie van de deelstaat Hessen gebruikt een door Palantir aangedreven systeem, *hessenDATA*, om uitgebreide individuele profielen van personen op te stellen. Het systeem kan gekende informatie over een persoon weergeven, zoals wanneer en waar ze zijn gecontroleerd door de politie, een overzicht van arrestaties, of ze ooit met drugs zijn betrapt en waar ze wonen.

In België gebruikt de federale politie een systeem met de naam ‘i-Police’. Dit systeem heeft allerlei functies, zoals:

- patronen analyseren en ‘voorspellen’;
- toekomstige misdrijven voorspellen met het oog op ‘preventie’;
- monitoring en toezicht mogelijk maken;
- politietoezicht, controles en fouillering toewijzen;
- en andere vormen van interventie en handhaving.¹¹⁶

De Belgische politie maakt ook profielen van personen en groepen en plaatst hen in specifieke databanken, een kwestie die hieronder uitgebreider wordt besproken. Dit

omvat ook het gebruik van deze databanken voor zogenoemde ‘stadsbendes’, een term vol racistische connotaties.¹¹⁷ Mensen die geprofileerd worden als vermeend ‘bendelid’, worden het doelwit van monitoring, toezicht en meer politiecontroles en fouilleringen.¹¹⁸

In Duitsland werden tools ingevoerd om criminaliteit bij individuen te ‘voorspellen’, en voor profilering en ‘risicobeoordeling’ om het zogenaamde toekomstige risico op zogenaamde islamitische¹¹⁹ terroristen of voorstanders van terrorisme te beoordelen. Het federale recherchebureau heeft twee individuele tools voor ‘risicobeoordeling’ ontwikkeld die RADAR genoemd worden (‘Rule-based Analysis of Potentially Destructive Offenders for the Assessment of Acute Risk’, [op regels gebaseerde analyse van potentieel destructieve overtreeders voor de beoordeling van acuut risico]).

Een van de varianten, RADAR-iTE, is een instrument dat wordt gebruikt om zogenoemde ‘islamisten’ te analyseren en profileren. De Belgische federale politie heeft verklaard dat zij een vergelijkbaar instrument als RADAR-iTE gebruikt.¹²⁰ Een andere variant, RADAR-rechts, wordt ingezet door het Duitse federale recherchebureau om personen met extreemrechtse opvattingen te profileren die als gewelddadige bedreiging worden beschouwd. De autoriteit ontwikkelt bovendien een aanvullend systeem: RADAR-Haft (“RADAR-detentie”), om de neiging tot geweld van gedetineerden bij hun vrijlating te beoordelen.

Zowel RADAR-iTE als RADAR-rechts zijn bedoeld om in de eerste plaats het risico te evalueren van personen die eerder zijn aangeduid als “Gefährder” (iemand die iemand of iets in gevaar brengt). Dit is een dreigingsclassificatie die is ontwikkeld door de Duitse politie en inmiddels binnen de hele EU wordt toegepast.¹²¹ De term is vaag omschreven en vatbaar voor subjectieve interpretatie. De systemen worden ook gebruikt om “relevante personen” te beoordelen. Dit is opnieuw een onduidelijk en subjectief begrip. De risicoprofielen die uit deze systemen voortkomen, worden gebruikt om individuen die zogezegd een ‘hoog-risico’ inhouden te identificeren en te prioriteren voor verdere handhaving en interventie.¹²²

In Spanje is VioGén een van de bekendste systemen voor individuele risicobeoordeling. Het doel van dit systeem is om het risico op gendergebaseerd geweld in te schatten voor een persoon die een incident heeft gemeld. De beoordeling bepaalt welke acties de politie vervolgens onderneemt.¹²³

De politie in Spanje gebruikt ook een meer ongebruikelijk type ‘voorspellend’ systeem. VeriPol is een algoritmisch systeem dat de Spaanse nationale politie inzette om zogenaamde valse aangiftes van misdrijven te detecteren. Het gebruikt technieken voor natuurlijke taalverwerking om de teksten van aangiftes van overvallen, zakkenrollerij en handtasdiefstal te analyseren. In de praktijk functioneert het als een soort leugendetector. Het systeem werd ontwikkeld om fraude door valse aangiftes te voorkomen. Het belangrijkste doel was om agenten snel een inschatting te geven of een misdaadaangifte mogelijk vals was.¹²⁴ In maart 2025

werd gemeld dat de nationale politie VeriPol niet meer gebruikte. Het Spaanse ministerie van Binnenlandse Zaken verklaarde dat dit kwam doordat het systeem niet voldoende rechtsgeldigheid had in gerechtelijke procedures.¹²⁵

Veiligheidsautoriteiten analyseren wereldwijd, ook in Europa, in toenemende mate zogenoemde 'Passenger Name Records' (PNR), gegevens van vliegtuigpassagiers. Dit zijn persoonlijke data die luchtvaartmaatschappijen verzamelen voor commerciële doelen wanneer iemand een vlucht boekt.¹²⁶ PNR-gegevens worden getoetst aan politiedatabanken en andere bestanden van de overheid. Er worden algoritmes gebruikt om systematisch patronen in deze gegevens te zoeken op basis van vooraf bepaalde criteria.¹²⁷ Dergelijke systemen draaien in feite het vermoeden van onschuld om, waardoor iedereen die met het vliegtuig reist als een potentiële verdachte wordt behandeld.¹²⁸ De EU is van plan het gebruik van deze systemen uit te breiden naar andere vormen van vervoer, te beginnen met reizen over zee.¹²⁹

In Spaanse gevangenissen wordt een systeem met de naam DRAVY gebruikt om gevangenen te identificeren die zogenaamd een proces van 'jihadistische' radicalisering doormaken.¹³⁰ Aangezien het hoofddoel van DRAVY is om 'jihadistische' radicalisering te beoordelen, is het systeem fundamenteel discriminerend, omdat het zich bijna uitsluitend richt op moslims en mensen met een moslimachtergrond. Het systeem is opgezet om 'jihadisme' aan te pakken, een begrip dat zelf gebaseerd is op discriminerende Westerse stereotypen.

Een vergelijkbaar instrument, RisCanvi, wordt ook gebruikt in Spaanse gevangenissen om het risico op recidive te 'voorspellen'. Dit systeem wordt gebruikt om beslissingen te nemen over voorwaardelijke invrijheidstelling, tijdelijke verloven en de classificatie van gevangenen.¹³¹

Gebruikte data

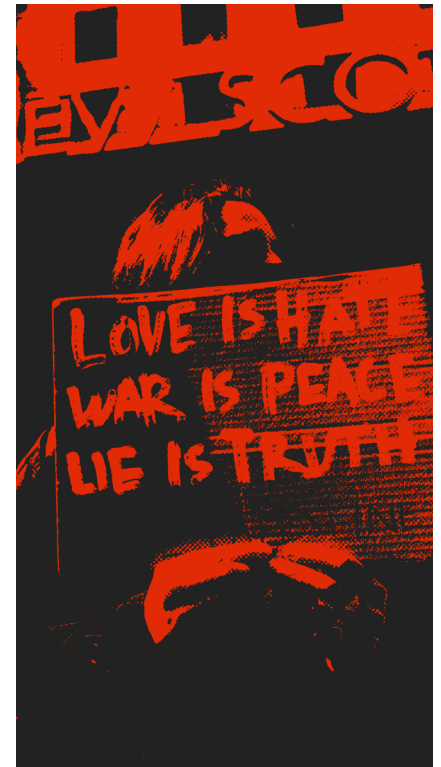
Deze systemen worden getraind, ontwikkeld en gebruikt met data afkomstig van de politie, wetshandhavingsinstanties en strafrechtelijke autoriteiten.

Deze autoriteiten verzamelen of hebben vaak toegang tot data uit een brede waaier aan bronnen. In Duitsland gebruiken de systemen van Palantir gegevens uit politiedatabanken en andere bronnen, waaronder sociale media. In de afgelopen jaren zijn er juridische stappen ondernomen tegen deze systemen en tegen de wetten inzake data-analyse die hun gebruik mogelijk maken.¹³² Toen één van deze juridische procedures erin slaagde om de reikwijdte van de analyses en gebruikte databronnen te doen beperken, verklaarde een bron bij de Duitse politie: "Er klonk gekreun toen het vonnis kwam en collega's zich realiseerden dat ze plots veel minder mochten doen."¹³³

Het Belgische i-Police-systeem heeft als doel om gegevens uit alle Belgische politiedatabanken en videobewakingsbeelden bij elkaar te brengen. Het gebruikt daarnaast open-source-'inlichtingen', zoals informatie van sociale media en persberichten. Om deze

functies te vervullen, gebruikt i-Police digitale technologieën afkomstig van verschillende onderaannemers, waaronder een aantal Israëlische bedrijven zoals Interionet en TA9/Rayzone. De CEO van TA9/Rayzone was eerder adjunct-directeur van Eenheid 8200, de inlichtingeneenheid van het Israëlische leger, die verantwoordelijk is voor de ontwikkeling en inzet van ‘Gospel’, een AI-systeem dat automatisch bombardementsdoelen genereert in Gaza, als onderdeel van Israël’s voortdurende genocide en massamoorden op de Palestijnen.¹³⁴

De gegevens die deze systemen gebruiken, zijn fundamenteel bevooroordeeld. Politiediensten in heel Europa focussen onevenredig op mensen met een als minderheid beschouwde etnische achtergrond. De politie in Spanje houdt bijvoorbeeld mensen onevenredig vaak tegen en fouilleert hen op basis van hun raciale, etnische of religieuze uiterlijk.¹³⁵ In Duitsland zijn niet-staatsburgers oververtegenwoordigd bij de verdachten van de politie, bij veroordelingen in de rechtbanken en bij mensen die een gevangenisstraf uitzitten.¹³⁶ Het Belgische strafrechtstelsel is herhaaldelijk veroordeeld wegens racistische praktijken, meer bepaald etnische profilering.¹³⁷ Het Committee on the Elimination of Racial Discrimination (CERD [Comité voor de Eliminatie van Rassendiscriminatie] van de VN is bezorgd over het feit dat mensen met een buitenlandse achtergrond oververtegenwoordigd zijn in het Belgische strafrechtstelsel, vooral in de gevangenissen.¹³⁸



De gegevens van de politie en het strafrechtstelsel die in deze digitale systemen worden gebruikt, zijn doordrenkt van structurele en institutionele vooroordelen, oververtegenwoordiging en discriminatie. Toch worden ze gebruikt om op data gebaseerde ‘voorspellende’, profilerings- en ‘risicobeoordelingssystemen’ te creëren, ontwikkelen en toe te passen. Hierdoor focussen ze steeds meer op dezelfde gemarginaliseerde groepen en gemeenschappen. De resultaten van deze operaties worden vervolgens opnieuw in de systemen ingevoerd, waardoor de kans toeneemt dat mensen uit die groepen en gemeenschappen in de toekomst opnieuw als ‘hoog risico’ worden beschouwd. Op die manier creëren deze algoritmen een zichzelf waarmakende voorspelling of feedbackloop. Er zijn duidelijke voorbeelden van hoe deze discriminerende gegevens de outputs van deze systemen beïnvloeden.

De volledige lijst van gegevens die het Duitse profileringssysteem RADAR-iTE gebruikt, is niet bekend. Het systeem vertrouwt echter op een beoordeling op afstand, zonder enig direct contact met de beoordeelde persoon.¹³⁹ De beoordeling omvat thema’s zoals “geweld tegen personen,” “interactie met autoriteiten en andere instellingen,” en “leger en reizen.” Andere vragen zijn bijvoorbeeld: “Hoe ziet zijn/haar privéleven eruit? Is de persoon

veeleer een eenzaat of maakt hij/zij deel uit van een groep? Heeft hij/zij contacten buiten de islamitische scene? Heeft hij/zij een job?”.¹⁴⁰

Dergelijke vormen van profilering betekenen dat iemand die vanuit een conflictgebied heeft gereisd, of die bepaalde reisroutes gebruikt voor toerisme of familiebezoek, als verdacht of als een ‘risico’ kan worden geprofileerd. Datapunten zoals kennissen, contacten of reispatronen kunnen duidelijk leiden tot discriminatie.¹⁴¹ De beoordeling van RADAR-iTE bevat bovendien andere zorgwekkende en potentieel discriminerende elementen met betrekking tot psychische gezondheidsproblemen en suïcidale neigingen.¹⁴²

Er waren ook problemen met de gegevens die werden gebruikt om het Spaanse systeem VeriPol te trainen, dat intussen niet meer gebruikt wordt en dat werd ingezet om valse aangiftes van misdrijven te detecteren. VeriPol werd getraind op aangiftes die bij de politie waren ingediend, en die handmatig door een agent als waar of echt werden ingedeeld. Niet al deze zaken waren echter afgehandeld. Er was dus geen objectieve of sluitende vaststelling dat ze waar of onwaar waren. Het model was daarom volledig opgebouwd op basis van de veronderstellingen van de politieagent die de aangiftes indeelde.¹⁴³ Het is opmerkelijk dat het minstens zeven jaar duurde voordat de Spaanse autoriteiten de problemen met het systeem erkenden en het gebruik stopzetten.

Het VioGén-systeem in Spanje zou voorspellen of iemand gendergerelateerd geweld zal ervaren. Het systeem gebruikte echter niet de daadwerkelijke getuigenissen van de vrouwen die de gevallen van gendergebaseerd geweld rapporteerden, maar de verslagen van politieagenten over de verklaringen van deze vrouwen. De risicoscore die toegekend wordt, is dus volledig afhankelijk van de beoordeling van de politieagenten.¹⁴⁴ Het systeem kan bovendien alleen gegevens verwerken van aangiftes die daadwerkelijk zijn gedaan.

Veel ervaringen met gendergebaseerd geweld worden echter niet gemeld, vooral niet door vrouwelijke migranten, vrouwen uit gemarginaliseerde en economisch kwetsbare groepen en vrouwen met kinderen. Samen met LGBTQIA+ personen en mensen met een beperking worden deze groepen het meest getroffen door structurele obstakels bij het aangeven van hun daders. Het systeem hield daarom geen rekening met de ervaringen van degenen die het meest gemarginaliseerd zijn in de samenleving.¹⁴⁵

De concepten waarop deze ‘voorspellende’, profilerings- en risicobeoordelingssystemen zijn gebaseerd, zijn bovendien fundamenteel bevooroordeeld. Dit probleem komt voort uit een gebrek aan duidelijkheid dat leidt tot subjectiviteit, of uit cultureel specifieke termen met een geracialiseerde lading.

In Duitsland worden vage termen zoals “Gefährder” (iemand die iemand of iets in gevaar brengt) en “relevante Person” (personen die een belangrijke rol zouden kunnen spelen) gebruikt om mensen te categoriseren die worden verdacht van het

plegen of ondersteunen van geweld. Deze termen zijn inmiddels gangbaar geworden bij de veiligheidsautoriteiten en de politie en worden in de RADAR-systemen gebruikt. Ze zijn echter niet wettelijk gedefinieerd en dus vaag en onwetenschappelijk. Dit betekent dat mensen subjectief worden geprofileerd, naar goeddunken van de autoriteiten en op inconsistente wijze. Dit ondermijnt de legitimiteit van het systeem volledig.

Deze problemen komen aan het licht wanneer de termen in de praktijk gebruikt worden. Duitse politiediensten zijn veel terughoudender geweest in het classificeren van rechtse extremisten als gevaarlijk dan zogenaamde ‘islamisten’. Nadat in 2011 de terroristische neonazistische organisatie NSU (Nationalsozialistischer Untergrund) werd ontmaskerd, werden bijvoorbeeld slechts vier leden van de groep als “Gefährder” geclassificeerd.¹⁴⁶

Er zijn ook andere problemen met de data die in deze systemen worden gebruikt. Het Belgische systeem i-Police brengt data uit meerdere bronnen met politiegegevens samen, waaronder ‘niet-gevalideerde’ informatie. Dit omvat niet-geverifieerde data uit politierapporten, vaak gekend of omschreven als politie-‘inlichtingen’, waaronder informatie over personen die niet zijn veroordeeld of officieel beschuldigd van een misdrijf. De voorzitter van de gegevensbeschermingsautoriteit die toezicht houdt op de Belgische politie, het COC, heeft ernstige bedenkingen bij het gebruik van deze data in het i-Police-systeem.¹⁴⁷

Systemen die potentiële criminele activiteit, toekomstige criminaliteit of ‘risico’ op criminaliteit beoordelen, geven een conceptuele verschuiving weer: van beoordeling op basis van daadwerkelijk bewijs van een handeling of betrokkenheid bij een handeling, naar een ongespecificeerd, abstract risico dat zich in de toekomst zou *kunnen* ontwikkelen, wat vaak enkel ingeschat wordt op basis van indirect bewijs. Dit geldt voor alle persoonsgerichte systemen.



Gevolgen en impact

Deze ‘voorspellende’, profilerings- en risicobeoordelingssystemen worden gebruikt om een brede waaier aan beslissingen van de politie en wetshandhaving te beïnvloeden, gaande van toezicht en monitoring tot aanhoudingen en ondervragingen, fouilleringen, huiszoekingen en zelfs arrestaties.

Het hessenDATA-systeem van de politie in de Duitse deelstaat Hessen maakt buitengewoon ingrijpend toezicht mogelijk. Hoewel het verondersteld werd om gebruikt te worden voor ‘ernstige’ of ‘georganiseerde’ misdaad of misdrijven gericht tegen de ‘staatsveiligheid’, werd het uitgebreid ingezet voor niet-gewelddadige criminaliteit. In 2022 werd gerapporteerd dat van de ongeveer 14.000 jaarlijkse zoekopdrachten in hessenDATA er zo’n 12.000 werden gecategoriseerd als ‘preventieve maatregelen’ tegen strafbare feiten.¹⁴⁸

De output van deze systemen wijst personen doorgaans een ‘risicoscore’ toe: laag, gemiddeld of hoog, of variaties daarop. Dit verwijst naar de veronderstelde mate van waarschijnlijkheid dat ze een strafbaar feit plegen of strafbaar gedrag vertonen.

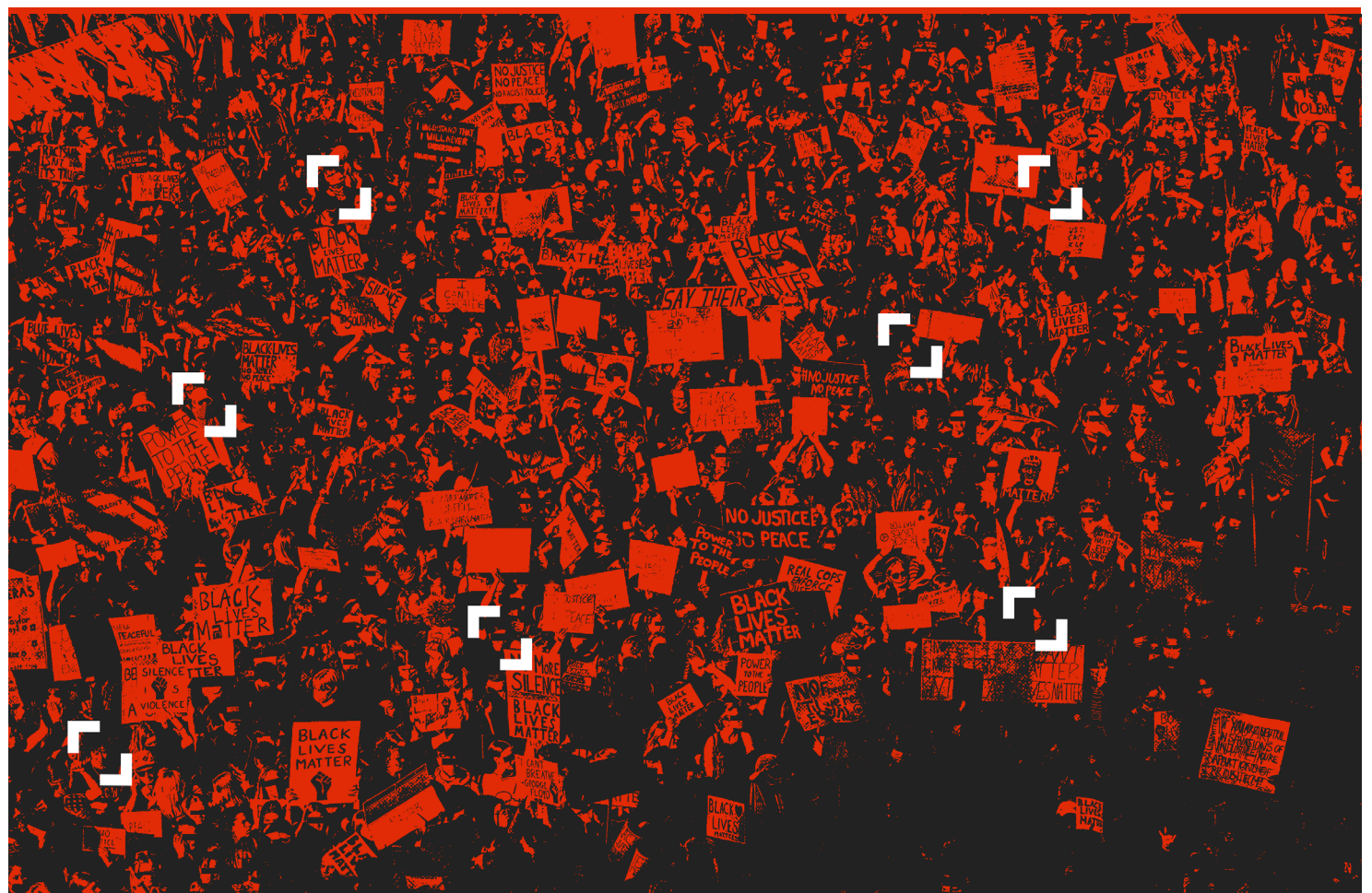
Volgens het Duitse federale recherchebureau werden sinds 2017 ongeveer 800 personen uit het ‘islamitische’ spectrum beoordeeld met RADAR-iTE.¹⁴⁹ Vanaf november 2023 werden 487 mensen geclassificeerd als ‘iemand die iemand of iets in gevaar brengt’ (“Gefährder”) in verband met ‘politiek gemotiveerde’ misdrijven op basis van religieuze ideologie. Het aantal extreemrechtse personen dat als “Gefährder” of “relevante persoon” wordt gecategoriseerd, blijft echter relatief laag, net zoals het aantal beoordelingen via het RADAR-rechts-systeem.¹⁵⁰

VioGén, het systeem dat de Spaanse politie gebruikt, is bedoeld om risicoscores toe te kennen, maar dan voor slachtoffers, niet voor daders. Een lage score betekent bijvoorbeeld dat de politie het slachtoffer telefonisch zal opvolgen, terwijl een score van extreem risico kan betekenen dat de politie het huis van het slachtoffer bewaakt of veiligheidspatrouilles inzet om de veiligheid van het slachtoffer te garanderen.¹⁵¹ In 95% van de gevallen volgen politieagenten de instructies van de risicoscore van VioGén.¹⁵²

Als gevolg van profilering op basis van gegevens van vliegtuigpassagiers (PNR) beschouwde het Duitse Federale Recherchebureau reisroutes tussen Turkije en Duitsland als potentieel verdacht. Deze worden z gezegd vaak gebruikt door ‘islamitische’ terroristen, “omdat ze ook populair zijn bij toeristen en dus goedkope prijzen en goede camouflagemogelijkheden bieden”.¹⁵³

Het DRAVY-systeem dat in Spaanse gevangenissen wordt gebruikt, voorspelt ten onrechte een hoog risiconiveau voor bijna de helft van de mensen die het beoordeelt.¹⁵⁴ Dit leidt ertoe dat deze personen zwaardere behandeling en strengere leefomstandigheden in de gevangenis ondergaan. Mensen die geen Spaanse onderdanen zijn, worden daarbij

onevenredig vaak gevisieerd.¹⁵⁵ Het RisCanvi-systeem, dat ook in Spanje wordt gebruikt, staat er eveneens om bekend te discrimineren op basis van sociaaleconomische status of omgaan met anderen. Het kent hogere risicoscores toe aan mensen met een geschiedenis van ‘onstabiel’ werk en een onzekere financiële situatie, aan mensen zonder familie of sociaal netwerk en aan mensen met familieleden of ouders met een strafblad.¹⁵⁶



Tegen september 2023 had VioGén ongeveer 770.000 zaken beoordeeld.¹⁵⁷ Miljoenen vliegtuigpassagiers worden geprofileerd via systemen voor PNR, gegevens van vliegtuigpassagiers. In 2022 stuurden 156 luchtvaartmaatschappijen in Duitsland ongeveer 424 miljoen PNR-gegevens door naar de politie. Ze hadden betrekking op ongeveer 121 miljoen passagiers. In 2023 werden tegen 31 oktober ongeveer 385 miljoen PNR-gegevens gegenereerd die betrekking hadden op 107 miljoen passagiers.

positieven (onjuiste overeenkomsten).¹⁵⁸ In de 8.284 gevallen van echte overeenkomsten (terecht-positieven) werden de volgende maatregelen genomen:

- 2.178 onderzoeken naar verblijfsstatus;
- 2.394 observaties of heimelijke controles door de politie;
- 1.236 arrestaties; 2.303 gerichte (openbare) controles; en
- 173 weigeringen aan de grens om het land binnen te komen.¹⁵⁹

Miljoenen passagiersgegevens worden dus geanalyseerd om enkele duizenden strafrechtelijke of immigratie-onderzoeken uit te voeren, waarvan de objectieve bewijskracht onbestaande of uiterst twijfelachtig is.

Individuele gevallen die in het rapport over Duitsland worden belicht, illustreren de extreme gevolgen wanneer iemand (ten onrechte) als een “Gefährder” wordt beschouwd. Vooroordelen tegen moslims zorgen ervoor dat moslimjongeren anders worden behandeld door politie en autoriteiten dan blanke jonge mannen met gelijkaardig problematisch gedrag. Ze worden waardoor sneller als een bedreiging beschouwd.¹⁶⁰

De gevolgen van profilering door RADAR-iTE zijn onder andere:

- onder toezicht en monitoring geplaatst worden.¹⁶¹
- ‘preventieve detentie’, van enkele dagen tot maanden;¹⁶²
- detentie voorafgaand aan deportatie,¹⁶³ en vervolgens deportatie.¹⁶⁴

De asielaanvragen van geprofileerde mensen worden soms ook tijdelijk stopgezet.¹⁶⁵

Andere op persoon gebaseerde systemen om criminaliteit te ‘voorspellen’ die in Europa worden gebruikt

Naast de hierboven genoemde voorbeelden gebruiken politie en strafrechtelijke autoriteiten in andere Europese landen ook op persoon gebaseerde ‘voorspellende’ en profileringstools. Eerder onderzoek heeft bewijs gevonden van soortgelijke systemen bij politiediensten en in gevangenissen in het Verenigd Koninkrijk, Italië en Nederland.

Amnesty International UK maakte onlangs bekend dat 11 politiediensten in het Verenigd Koninkrijk op het individu gerichte of individuele tools gebruikten om criminaliteit te ‘voorspellen’ of voor profilering.¹⁶⁶ Dit omvat:

- De ‘Violence Harm Assessment’ van de London Metropolitan Police, die individuen in Londen profileert op basis van het risico op gewelddadigheid. Vanaf augustus 2024 was 66% van de door het systeem geprofileerde personen zwart en slechts 22% blank;

- Het systeem ‘Integrated Offender Management’ (IOM) van de West Midlands Police, dat het potentieel voorspelt van individuen om in de toekomst schade te berokkenen. De interne analyse van de politie toonde aan dat zwarte mensen 2,4 keer meer kans hebben om in de ‘voorspelde’ groep met hoog risico te vallen dan een Noord-Europees (blank) persoon.

In Engeland en Wales gebruiken gevangenis- en reclasseringsdiensten het Offender Assessment System (OASys) om het risico op recidive te ‘voorspellen’ voor iedereen die in het strafrechtstelsel terechtkomt. Dit systeem kreeg veel kritiek wegens etnische profilering, bedreigingen van de privacy en het ontbreken van mogelijkheden voor verantwoording of herstel.¹⁶⁷

In Nederland heeft de politie een systeem gebruikt, ProKid, om het risico op recidive bij kinderen en jongeren te ‘voorspellen’.¹⁶⁸ In Amsterdam heeft de politie twee profileringsinstrumenten gebruikt, Top400 en Top600, die proberen de ‘top 600’ en ‘top 400’ van jongeren te profileren bij wie z gezegd de kans het grootst is dat ze verschillende soorten misdrijven zullen plegen.¹⁶⁹

Diana Sardjoe, een moeder van wie de zonen werden geprofileerd door Top400 en Top600, zei dat de systemen ertoe leidden dat haar zonen voortdurend werden gevolgd en lastiggevallen door de politie. Ze riep op tot een verbod op systemen voor ‘predictive policing’.¹⁷⁰

In Italië heeft de politie in het verleden een profileringsstelsel gebruikt, Delia, dat gebruik maakte van etnische gegevens om individuen te profileren.¹⁷¹





Videobewakingssystemen met AI

Politiediensten in Europa gebruiken steeds vaker videobewakingssystemen met AI. Deze systemen gebruiken op AI gebaseerde methoden om videomateriaal te doorzoeken, zoals beelden van CCTV-camera's en politiedatabanken, om mensen en voorwerpen te identificeren of 'verdacht' gedrag te detecteren.

Het onderzoek dat ten grondslag ligt aan dit rapport bevat voorbeelden van videobewakingssystemen met AI die politiediensten in België en Spanje gebruiken. *La Quadrature du Net* heeft daarnaast uitgebreid onderzoek gedaan naar het gebruik van videobewaking met AI door de politie in Frankrijk.¹⁷² In Duitsland identificeerde *AlgorithmWatch* twee pilootprojecten voor videobewakingssystemen met AI in gevangenissen, bedoeld voor 'zelfmoordpreventie'. Er is ook bewijs dat politiediensten in Italië videobewaking met AI gebruiken.

Het gebruik van videobewaking met AI door rechtshandavingsinstanties roept ernstige vragen op over schendingen van grondrechten, waaronder het recht op privacy en non-discriminatie.

Politiewerk

In Spanje gebruiken verschillende gemeenten in Madrid videobewakingssystemen met AI-methoden voor beeldherkenning. De systemen, geleverd door Bosch Security via het Amerikaanse bedrijf Intelligent Security Services, dienen twee doelen: automatische nummerplaatherkenning (automatic number plate recognition, ANPR) en de identificatie van criminele verdachten.¹⁷³ Het systeem kan ook worden gebruikt om mensen te zoeken op basis van kenmerken zoals haarkleur, kledij, gelaatskenmerken en leeftijd. Er is geen concreet bewijs dat het systeem de misdaadcijfers verlaagt.¹⁷⁴ In Madrid waren er in januari 2025 minstens 83 videobewakingscamera's met AI in gebruik bij de gemeentepolitie, met plannen om er nog eens 38 te installeren.¹⁷⁵

In België gebruiken de lokale politiediensten en de federale politie verschillende videobewakingssystemen met AI. Dit omvat software van BriefCam, een bedrijf uit Israël, voor retrospectieve beeldanalyses door videosamenvattingen.¹⁷⁶ Net zoals het systeem van Bosch in Spanje kan de politie met dit systeem mensen indelen op basis van criteria zoals kledijkleur, geslacht of bezittingen.

Deze laatste functie zou in strijd met de wet kunnen zijn. Het Belgische wettelijke kader inzake non-discriminatie staat gerichte onderzoeken toe op basis van objectieve criteria, maar verbiedt het massaal sorteren van individuen. Op basis van deze en andere voorbeelden roept het Belgische rapport op om de geplande videobewaking met AI in het enorme i-Police-project te laten vallen.

In 2023 werd Frankrijk het eerste Europese land dat biometrisch toezicht legaliseerde, in de vorm van algoritmische videobewakingssystemen, onder een wet inzake de organisatie van de Olympische Spelen van Parijs 2024.¹⁷⁷ Het systeem werd ingezet in Saint-Denis, een voorstad met een grotendeels als minderheid beschouwde etnische bevolking en mensen uit de arbeidersklasse in het noorden van Parijs, waar een groot deel van de Olympische Spelen plaatsvond.¹⁷⁸ Het systeem was oorspronkelijk wettelijk toegestaan tot eind 2024, maar zodra de Olympische Spelen voorbij waren, probeerden de autoriteiten het gebruik ervan te verlengen.¹⁷⁹

Elders in Frankrijk streed *La Quadrature du Net* drie jaar lang in de rechtbanken tegen de invoering van videobewakingssoftware met AI, namelijk Briefcam, in Moirans in de Isère. Op 30 januari 2025 oordeelde een rechtbank dat het gebruik van dit systeem onwettig was: het schond meerdere onderdelen van de bescherming van de privacy onder de verordening inzake gegevensbescherming van de EU en de Franse Interne Veiligheidscode.¹⁸⁰

De uitspraak maakt de wettelijke kaders ongeldig die eerder geautomatiseerde videobewakingssystemen toestonden, ook diegene die via tijdelijke experimentele

vergunningen voor de Olympische Spelen van Parijs 2024 waren ingevoerd. De uitspraak vormt ook een belangrijk juridisch precedent voor lopende rechtszaken tegen algoritmische systemen die de politie in Frankrijk gebruikt.¹⁸¹

Gevangenen

In Duitsland identificeerde *AlgorithmWatch* twee pilootprojecten voor videobewakingssystemen met AI in gevangenen, bedoeld voor ‘zelfmoordpreventie’. Deze dystopische bewakingssystemen zouden de bestaande videobewaking in gevangencellen aanvullen met machinaal erende algoritmen om zo vroege signalen van zelfmoordpogingen te detecteren.

In Noordrijn-Westfalen probeerden het ministerie van Justitie en het Duitse IT-bedrijf FusionSystems een machinaal lerend algoritme te ontwikkelen gebaseerd op trainingsbeelden die door acteurs/actrices waren gemaakt. Het algoritme werd getraind om voorwerpen (bijv. messen, scharen, touwen, aanstekers) en gedrag te detecteren dat op zelfmoordintenties kan wijzen. Voorbeelden hiervan zijn een strop van een riem maken, een touw knopen of een strop vastmaken aan het raamrooster, een mes nemen of spelen met een groot mes. Het algoritme werd ook getraind met beelden van onopvallend gedrag zoals hurken, lezen of televisie kijken. Dit was bedoeld om het systeem te leren om een onderscheid te maken tussen onschuldige situaties en aanwijzingen van een risico op zelfmoord.¹⁸² Het systeem integreerde naar verluidt ook skelettracking, waarbij sensoren en machinaal lerende technieken worden gebruikt om de bewegingen van gewrichten en lichaam van een persoon te volgen.¹⁸³

Deze factoren zouden worden gebruikt om een ‘gevaarlijkheidsniveau’ toe te kennen aan de situatie in de cel. Dat zou voortdurend opnieuw berekend worden. Bewakers/bewaaksters in de gevangenis zouden via een visueel alarmsysteem met ‘verkeerslicht’ op de hoogte worden gehouden van de actuele situatie. Ze horen een geluid wanneer de situatie ‘erg gevaarlijk’ is, zodat er snel kan ingegrepen worden.

In Nedersaksen proberen het FZI Research Centre for Innovation Technology en het IT-beveiligingsbedrijf VOMATEC Innovations een soortgelijk systeem te ontwikkelen. Het doel is om “operationele software als prototype” te produceren. Die zal waarschijnlijk eerst in een gevangenis in Oldenburg ingevoerd worden.¹⁸⁴

Aanvankelijk zou het project bewakingstechnologie met AI gebruiken in gemeenschappelijke ruimtes, zoals buiten of in recreatieruimtes. Dit moest bijvoorbeeld het “overdragen van verboden voorwerpen tussen gevangenen” identificeren.¹⁸⁵ Dit werd echter zwaar bekritiseerd door de gegevensbeschermingsautoriteit van Nedersaksen.¹⁸⁶ In tegenstelling tot het systeem in Noordrijn-Westfalen, dat getraind werd met beelden van acteurs, wordt het systeem in Nedersaksen getraind met echte opnames van zelfmoordpogingen en geweld in

gevangenissen.¹⁸⁷

Er is grote bezorgdheid over het gebruik van op AI gebaseerde systemen om emoties of lichaamsbewegingen te analyseren. De technologie is niet alleen wetenschappelijk niet bewezen,¹⁸⁸ maar ook gevoelig voor raciale of etnische vooroordelen. Het is mogelijk dat de cameratechnologie enkel voor een lichtere huidskleur gekalibreerd is. De gezichtsuitdrukkingen van zwarte mannen worden vaker geïnterpreteerd als “agressief” dan die van blanke mannen.¹⁸⁹ Culturele vooroordelen kunnen de normatieve interpretatie van lichaamstaal of gezichtsuitdrukking beïnvloeden. Andere factoren die deze technologie kunnen beïnvloeden zijn slechte belichting of gezichten die worden verborgen of er anders uitzien door een bril of hoofddoek.

Aangezien valse negatieven mogelijk levensbedreigende gevolgen kunnen hebben, is het toekomstig gebruik van deze systemen buitengewoon zorgwekkend. Zelfs als ze werken zoals bedoeld, en dus voldoende nauwkeurig zijn, zijn ze zeer ingrijpend¹⁹⁰ en dringen ze diep door in de privacy van mensen in de gevangenis. Een voormalig gevangene, geïnterviewd door *AlgorithmWatch*, verklaarde dat werkelijk effectieve zelfmoordpreventie de afschaffing van het gevangenisstelsel vereist:

“De gevangenis is geen therapeutische plek. De gevangenis is niet bedoeld voor rehabilitatie, maar voor straf. Er is dus geen hulp voor mensen die het nodig hebben, het is erg deprimerend en ik zie dat mensen het niet lang volhouden... Er zijn ook andere manieren om zelfmoord te voorkomen: door therapie en empathie, door gemeenschappelijke steun, door mensen te helpen een doel in hun leven te vinden.”¹⁹¹

In Spanje startte het ministerie van Justitie in 2023 met een proefproject in de gevangenis Mas d'Enric in de buurt van Tarragona met “gezichtsherkenning en video-analysecamera's” voor “realtime detectie van non-verbale uitdrukkingen en houdingen die wijzen op illegaal gedrag”. Dit project werd deels gefinancierd door de Europese Unie. Het was de bedoeling dit uit te breiden naar andere gevangenissen in de regio. De Catalaanse overheid kondigde echter in januari 2024 aan dat, gezien de recent aangenomen wet inzake AI, het project niet zal worden voortgezet.¹⁹²



Databanken

Databanken leveren vaak de data die gebruikt worden in ‘voorspellende’, profilerings- en ‘risicobeoordelingssystemen’ van politie en strafrechtelijke autoriteiten. Ze kunnen ook dienen als rechtvaardiging of vermeende bewijsgrond voor politieoptreden en handhavingsmaatregelen. Ze bestrijken heel wat bevolkingsgroepen en kunnen enorme hoeveelheden gevoelige informatie bevatten, variërend van biografische gegevens tot vingerafdrukken, foto’s en strafbladen, naast vele andere zaken.

In België bestaan er verschillende categorieën databanken die de politie en wetshandhaving gebruiken:

- de Algemene Nationale Gegevensbank wordt gebruikt voor politieonderzoeken;
- standaard databanken bestaan uit politierapporten en ‘inlichtingen’;
- speciale databanken worden opgezet door de politie voor specifieke doelen, zoals zogenaamde ‘stadsbendes’;
- gemeenschappelijke databanken delen gegevens tussen politie en inlichtingendiensten voor vermeende terrorismebestrijding; en
- technische databanken bevatten automatisch verzamelde gegevens, zoals die van camera’s voor automatische nummerplaatherkenning.¹⁹³

TAJ ('Traitement d'Antécédents Judiciaires'), voor de dagelijkse activiteiten van de wethandhavingsdiensten. De Franse autoriteiten hebben geprobeerd die te koppelen aan verschillende andere databanken.¹⁹⁴ Deze databank bevat uitgebreide informatie over mensen die ervan verdacht worden een ernstig misdrijf gepleegd te hebben, en ook slachtoffers van strafbare feiten.¹⁹⁵ Bij de gemeentelijke politiediensten in Frankrijk is het illegaal verzamelen van gegevens een veelvoorkomende praktijk.¹⁹⁶

De *Police Nationale* en de *Gendarmerie* zijn gemachtigd om de TAJ-databank te gebruiken voor post-factum gezichtsherkenning in het kader van gerechtelijke onderzoeken. Dit betekent dat zij bijvoorbeeld beelden van bewakingscamera's of foto's van verdachten kunnen gebruiken om in de databank te zoeken naar overeenkomende registraties. De functie voor gezichtsvergelijking wordt ook steeds vaker ingezet voor administratieve identiteitscontroles. Gemiddeld wordt het systeem meer dan 1.600 keer per dag voor dit doel gebruikt.¹⁹⁷

De Spaanse politiedatabank over buitenlandse onderdanen, ADEXTTRA, bevat een uitgebreide lijst met achtergrondinformatie. Dit omvat:

- nationaliteit;
- burgerlijke staat;
- beroep en werk;
- eigendommen;
- inkomen en opbrengsten;
- informatie over samenwonen;
- informatie over gedrag, detentie en buitengerechtelijke vrijheidsberovingen en strafblad;
- foto's en ander beeldmateriaal;
- vingerafdrukken; en
- stemopnames.¹⁹⁸



De databanken die de politie en wetshandavingsinstanties in Europa gebruiken, bevatten enorme hoeveelheden gegevens. De Belgische Algemene Nationale Gegevensbank bevat informatie over drie miljoen mensen, een kwart van de Belgische bevolking.

In Frankrijk bevat de TAJ-databank bijna 20 miljoen individuele registraties en ongeveer 10 miljoen foto's van gezichten.¹⁹⁹ De databank *Titres électroniques sécurisés* (TES, of

Beveiligde Elektronische Documenten), opgericht in 2016 door het ministerie van Binnenlandse Zaken, bevat gegevens over alle aanvragers van identiteitskaarten en paspoorten.²⁰⁰ Uiteindelijk zou het Franse ministerie van Binnenlandse Zaken toegang kunnen krijgen tot een afbeelding van het gezicht van iedereen die op Frans grondgebied verblijft.²⁰¹ Dit sluit naadloos aan bij de plannen van de EU om ‘identiteitsgegevens’ te verzamelen over elke buitenlandse burger die zich op EU-grondgebied bevindt en die beschikbaar te stellen aan politie- en immigratieautoriteiten.²⁰²

Honderden gemeentelijke Franse politiekorpsen zijn uitgerust met de software ‘Smart Police’, een platform en digitale applicatie waarmee ze onderweg rapporten kunnen opstellen, foto’s kunnen nemen en gebeurtenissen kunnen beschrijven. Dit wordt vervolgens in de relevante centrale databanken opgenomen. Smart Police bevat een ‘voorspellend’ element dat informatie uit verschillende bronnen bundelt, gaande van politiegegevens over misdrijven en locatiegegevens van agenten tot sociaaleconomische gegevens van de bevolking, weersvoorspellingen en ‘geruchten’ van schooldirecteuren, huisbazen en zelfs sociale media, om zo te proberen het risico op crimineel gedrag te ‘voorspellen’.²⁰³

De gegevens in deze databanken en de manier waarop ze worden gebruikt, kunnen ernstige en verstrekende gevolgen hebben. Ze bevatten grote hoeveelheden onjuiste informatie, evenals niet-geverifieerde informatie die wordt voorgesteld als ‘inlichtingen’.

Onjuiste gegevens lijken misschien onschuldig, maar kunnen serieuze gevolgen hebben. Als bijvoorbeeld verouderde informatie over een persoon in een databank blijft staan, kan dit leiden tot onterechte arrestaties. In Spanje werden migranten al ten onrechte vastgehouden omdat hun gegevens in de databanken niet correct waren bijgewerkt.²⁰⁴

Naast feitelijk correcte informatie kunnen zogenoemde politie-inlichtingen worden gebruikt in ‘voorspellende’ en profileringsystemen. Deze beïnvloeden de uitkomsten van het systeem, die op hun beurt de beslissingen van politie en andere autoriteiten beïnvloeden. Zo wordt niet-geverifieerde informatie omgezet in feiten, die vervolgens tegen mensen kunnen worden gebruikt.

Databanken zijn ook zorgwekkend door onwettige discriminatie. Ze kunnen op zichzelf al discriminerend zijn, vanwege de herkomst en aard van de opgenomen gegevens. Het gebruik ervan kan ook leiden tot discriminerende praktijken.²⁰⁵ Gemarginaliseerde mensen, groepen en gemeenschappen die historisch zijn gevisieerd, gecontroleerd en bestraft door overheidsinstanties zijn aanzienlijk oververtegenwoordigd in de databanken van de politie en het strafrechtelijke systeem. Dit omvat zwarte en geracialiseerde mensen en gemeenschappen, migranten, mensen uit de arbeidersklasse of sociaaleconomisch achtergestelde milieus, queer personen en mensen met psychische problemen.²⁰⁶ Verschillende Duitse deelstaten hebben databanken bijgehouden met labels zoals “junkie”, “zwerver”, “zigeuner” en “besmettelijk” (dat laatste in relatie tot mensen met hiv).²⁰⁷

Een groeiend aantal werkgevers en autoriteiten gebruikt Belgische politiedatabanken voor veiligheidsscreenings. Mensen van Noord-Afrikaanse en Belgisch-Marokkaanse afkomst zijn oververtegenwoordigd onder degenen die deze screenings niet doorstaan. Het rapport over België beschrijft ook het verhaal van een jonge moslimman die werd uitgesloten van werk vanwege onjuiste informatie in een politiedatabank.²⁰⁸

Lokale politiekorpsen in België staan er ook om bekend databanken op te zetten om zogenaamde ‘stadsbendes’ te viseren. Dit is een term die sterk beïnvloed wordt door racistische percepties van jonge mannen. De voorstelling van deze groepen als zowel ‘stads’ als ‘bende’ is gebaseerd op hun etniciteit. De criteria voor opname in deze databanken waren vaag. Mensen die op deze lijsten stonden, werden het doelwit van monitoring, toezicht en verhoogde identiteitscontroles en fouilleringen.²⁰⁹

De lokale politie in België houdt ook databanken bij over sekswerker(sters). Deze worden ogenschijnlijk gebruikt om de sector te ‘reguleren’, maar maken het in werkelijkheid mogelijk om sekswerker(sters) te monitoren en te volgen. Omdat registratie voor sekswerker(sters) verplicht is, sluit dit mensen met een onzekere of irreguliere migratiestatus uit en drijft dit hen weg van netwerken van steun en veiligheid.²¹⁰

De Spaanse ADEXTTRA-databank wordt gebruikt om migranten te identificeren en hun verblijfsstatus te controleren. De politie kan zo gemakkelijker de identiteit controleren van mensen die als ‘buitenlands’ worden waargenomen. Er is overvloedig aangetoond dat de Spaanse politie zich schuldig maakt aan etnisch profileren.²¹¹

Er zijn zwakke beperkingen en waarborgen rond het gebruik van deze databanken en de informatie die ze bevatten door de politie. De handhaving ervan is zwak. Politieagenten die illegaal toegang krijgen tot gegevens of de vereisten of richtlijnen overtreden, worden vaak niet gerapporteerd of bestraft.²¹² Ook worden de bewaartermijnen van gegevens vaak overschreden, wat resulteert in feitelijk onbeperkte opslag van persoonsgegevens en mogelijk gevoelige gegevens, zonder verwijdering.²¹³ De politie verwijdert gegevens die zij wettelijk verplicht is te wissen niet. Er zijn weinig tot geen handhavingsmechanismen of sancties wanneer dit gebeurt.²¹⁴



Conclusie

Dit rapport heeft een overzicht gegeven van de manieren waarop de politie en strafrechtelijke instanties in Europa ‘voorspellende’ systemen ontwikkelen, gebruiken en inzetten, met een bijzondere focus op België, Frankrijk, Duitsland en Spanje. Dit omvat systemen voor het ‘voorspellen’ van criminaliteit en voor profilering, andere geautomatiseerde, door data gestuurde systemen en systemen voor data-analyse. Het rapport heeft ook politie-databanken en de videobewakingssystemen met AI geanalyseerd die de politie en gevangenisautoriteiten gebruiken.

Het rapport toont een duidelijke trend aan waarbij politiediensten in toenemende mate ‘voorspellende’, profilerende en andere op data gebaseerde besluitvormingssystemen implementeren. Deze systemen worden vaak aangekocht bij de technologie-industrie voor toezicht, waaronder bedrijven die bekritiseerd zijn vanwege hun banden met de Israëlische staat.

Het gebruik van systemen om criminaliteit te ‘voorspellen’ roept ernstige vragen op over toegenomen criminalisering, bestraffing (inclusief straffen buiten het strafrecht om) en discriminatie van gemarginaliseerde individuen en gemeenschappen, vooral geracialiseerde mensen en mensen uit economisch achtergestelde groepen.

Het rapport stelt zich ook vragen over de nauwkeurigheid van deze systemen, over het gebrek aan transparantie en betekenisvolle verantwoording en over de wettelijkheid. Daarom steunen de auteurs van dit rapport de oproepen van onderzoekers en partnerorganisaties in België, Frankrijk, Duitsland en Spanje tot een verbod op alle vormen van het gebruik van AI en algoritmes in de rechtshandhaving en het strafrecht, en eveneens tot strikte eisen op het vlak van transparantie en verantwoording.

Discriminatie

Op locatie gebaseerde ‘voorspellende’ systemen bevatten geen gegevens over specifieke individuen. Toch zijn het vooral geracialiseerde individuen en mensen uit meer achtergestelde wijken die onderworpen worden aan politiecontroles, fouillering en eventuele gevolgen in de gebieden waar misdaad ‘voorspeld’ wordt.

De voorspellingen leiden tot een verhoogde politieaanwezigheid in deze wijken en controle op de mensen en gemeenschappen die er wonen. Dit leidt tot etnische profilering, controles en het fouilleren van mensen in die zones, en uiteindelijk tot criminalisering. Op die manier bieden systemen die criminaliteit ‘voorspellen’ de rechtvaardiging voor het racistisch viseren van bepaalde wijken en hun bewoners. Bovendien omzeilt dit de zogenaamde wettelijke bescherming tegen etnische profilering.

Deze politiecontroles, interventies en incidenten worden vervolgens geregistreerd in de databanken die de ‘voorspellende’ systemen voeden. Het gebruik van deze gegevens voor verdere ‘voorspellingen’ creëert een feedbackloop waarbij steeds dezelfde wijken en profielen keer op keer worden gevisieerd.

Hetzelfde probleem met bevooroordeelde data die leiden tot bevooroordeelde uitkomsten en zichzelf versterkende feedbackloops doet zich voor bij op de persoon gebaseerde voorspellende systemen. Het Spaanse DRAVY-systeem vertoont eveneens een fundamentele vorm van discriminatie in het ontwerp: het focust op het westerse concept van zogenaamde ‘jihadistische’ radicalisering en richt zich daardoor bijna uitsluitend op moslims en mensen met een moslimachtergrond. Het systeem kent bovendien een aanzienlijk aantal vals-positieven. Het Duitse systeem RADAR-iTE is dan weer gebaseerd op islamofobie en een bevooroordeelde opvatting van wie als een potentiële ‘dreiging’ wordt beschouwd. Dit resulteert in aanzienlijke vooroordelen ten opzichte van moslims in de uitkomsten van het systeem en qua personen waarop dit een impact heeft.



Criminalisering

Binnen op locatie gebaseerde systemen om criminaliteit te ‘voorspellen’ worden hele buurten bestempeld als crimineel, en wordt ‘voorspeld’ dat daar vaak en veel misdrijven zullen plaatsvinden. Dit leidt tot verhoogde politieaanwezigheid en gerichte acties zoals patrouilles, fouillering, identiteitscontroles en andere operaties. Het biedt ook een rechtvaardiging voor feitelijk willekeurige handelingen zoals tegenhouden, identiteitscontroles en fouilleringen, zonder concrete verdenking. De ‘voorspelling’ fungeert als rechtvaardiging en als verdenking. Dit vergroot de kans op criminalisering van de mensen en gemeenschappen die in die gebieden wonen en werken. Dat kan gebeuren zonder enig objectief bewijs van strafbaar gedrag.

Op de persoon gebaseerde systemen profileren mensen op basis van hun achtergrond, waarbij ze rechtstreeks als crimineel worden bestempeld of onrechtstreeks gestigmatiseerd worden als potentieel crimineel. Deze mensen worden vervolgens beschouwd en behandeld alsof ze schuldig zijn, tot het tegendeel is bewezen. Profileringsystemen hebben er ook toe geleid dat mensen gelinkt worden aan anderen die zelf als crimineel geprofileerd zijn. Zo ontstaat een bijzonder breed net van criminalisering.

Individuele ‘voorspellingen’ of profielen kunnen leiden tot ernstige gevolgen binnen én buiten het strafrecht. Zoals dit rapport heeft samengevat, zijn bekende gevolgen onder meer toezicht en monitoring door politie of andere handhavingsdiensten, bezoeken aan huis of op het werk, huiszoekingen, uitsluiting van werkgelegenheid, ondervragingen, arrestaties en zelfs ‘preventieve’ detentie. De verblijfsstatus van mensen wordt onderzocht. Ze kregen te maken met grenscontroles en ondervragingen. Dit leidde tot weigering van toegang tot het grondgebied. Asielaanvragen werden gepauzeerd of stopgezet. Sommige mensen werden zelfs gedeporteerd. Dat kan gebeuren zonder enig objectief bewijs van strafbaar gedrag, enkel en alleen op basis van op data gebaseerde verdenking, gegenereerd door algoritmen.



Transparantie en verantwoording

Het gebrek aan transparantie rond de ontwikkeling, training en operationele inzet van deze ‘voorspellende’ systemen en profilerings- en risicobeoordelingssystemen vormt een fundamentele belemmering voor rechtvaardigheid en verantwoording.

Mensen die door de politie of wetshandhaving geïdентificeerd worden als gevolg van ‘predictive policing’ of systemen om criminaliteit te ‘voorspellen’, zijn zich daar vaak niet van bewust. De autoriteiten die deze systemen gebruiken, geven doorgaans geen informatie over deze systemen of de manier waarop ze deze inzetten. Ook worden mensen niet op de hoogte gebracht van het feit dat ze onderworpen zijn aan profilering, voorspelling of risicobeoordeling, of dat het optreden tegen hen daardoor beïnvloed werd. Dit roept ernstige vragen op over de eerlijkheid en onpartijdigheid van deze systemen en de processen waarop ze een invloed hebben.

Wettelijk kaders in Europa verplichten niet tot wezenlijke transparantie over deze systemen. Ook de aankomende verordening betreffende AI van de EU bevat geen echte verplichtingen rond transparantie in deze context. Er zijn aanzienlijke uitzonderingen voorzien voor systemen die worden gebruikt om strafbare feiten op te sporen, te voorkomen, te onderzoeken en te vervolgen.

Dit moet veranderen. Politiediensten en strafrechtelijke autoriteiten moeten de details publiceren van alle door data gestuurde, algoritmische of geautomatiseerde systemen die zij gebruiken. Dit moet gebeuren via een publiek toegankelijke databank of website. Deze informatie moet onder meer het volgende omvatten: details over het systeem of de software en hoe dat systeem of die software werkt, welke gegevens worden gebruikt, op welke manier het systeem analyses uitvoert of resultaten genereert en waarvoor deze worden gebruikt en de mogelijke gevolgen ervan.

Wanneer een individu of groep te maken heeft met gelijk welke vorm van politieoptreden of strafrechtelijke gevolgen als gevolg van een geautomatiseerd besluitvormingssysteem of op data gebaseerde analyse, moeten zij daarvan op de hoogte worden gebracht. De politie of strafrechtelijke autoriteit moet het individu informeren en uitleg geven over hoe deze beslissing of uitkomst kan worden aangevochten.



Deze informatie moet verstrekt worden in een formaat en op zodanige manier dat individuen zonder expertise of kennis van deze systemen dit kunnen begrijpen.

Mensen en groepen moeten duidelijke mogelijkheden hebben om de resultaten of gevolgen van dergelijke geautomatiseerde beslissystemen aan te vechten, met reële kansen op verhaal.

Geen wettelijke basis en onwettelijk gebruik

Vele van deze controversiële systemen worden ontwikkeld, getest en gebruikt zonder voldoende wettelijke basis voor het gebruik. In vele gevallen werken ze zonder wettelijke basis. In sommige gevallen bleken ze onwettig te zijn, zoals in Duitsland. Ook de gegevensverzameling die aan de basis ligt van deze systemen wordt in bepaalde gevallen als onwettig beschouwd, zoals bijvoorbeeld in Frankrijk het geval was.

Onnauwkeurigheid

In veel gevallen zijn deze systemen fundamenteel onnauwkeurig. Ze leveren ernstige fouten of vals-positieve resultaten op, waardoor onschuldige mensen mogelijk onterecht geïdентificeerd worden. In veel gevallen hebben politie, wetshandhaving of andere autoriteiten deze systemen niet zinvol of grondig geëvalueerd vóór ze die zijn beginnen te gebruiken. Zelfs wanneer er wel tests zijn uitgevoerd, worden systemen met gebrekkige nauwkeurigheid soms toch verder gebruikt.

Nauwkeurigheid is op zich echter geen oplossing. Een ‘nauwkeurig’ systeem zou simpelweg de discriminatie bevestigen en versterken die al vervat zit in de data waarop het gebaseerd is.

Verbod

Zoals aangetoond in dit rapport, leiden de op locatie gebaseerde en op het individu gebaseerde ‘voorspellende’ systemen en systemen voor profilering en risicobeoordeling tot raciale en sociaaleconomische profilering, discriminatie en criminalisering.

Het gebruik heeft onrechtvaardige en discriminerende gevolgen, gaande van toezicht, identiteitscontroles en fouilleringen tot pesterijen door de politie, arrestatie, detentie en deportatie.

De conclusie van dit rapport en van de onderliggende analyses is



duidelijk: deze systemen moeten worden verboden.

De nationale wetgevers van landen waar deze systemen worden gebruikt, zouden een wettelijk verbod op het gebruik moeten invoeren. Ook zouden lokale overheden of gemeenteraden waar deze systemen worden ingezet, zoals steden of lokale besturen, moeten streven naar een verbod binnen hun eigen bevoegdheid.²¹⁵

Er lopen momenteel en al langere tijd campagnes tegen het gebruik van deze systemen in Europa en daarbuiten, zoals de campagne om systemen voor predictive policing te verbieden in de verordening betreffende AI van de EU,²¹⁶ de *Technopolice*-campagnes in Frankrijk²¹⁷ en België,²¹⁸ de coalitie *Safety Not Surveillance* in het VK²¹⁹, en *Stop LAPD Spying* in de VS.²²⁰ Het is essentieel om deze campagnes en gelijkaardige initiatieven te steunen nu overheden, politiediensten, gerechtelijke autoriteiten en bedrijven het gebruik van algoritmische en geautomatiseerde systemen en AI-systemen proberen uit te breiden.



“

The authors of this report support the calls of the researchers and partner organisations in Belgium, France, Germany and Spain for a prohibition on all uses of AI and algorithms in law enforcement and criminal legal settings, as well as strict transparency and accountability requirements.



Beeldkredieten

Voorpagina: [“Politie doet handboeien om”](#)
by Shirley de Jong

Pagina 6: [“Brussels police \(1\)”](#) by Eoghan OLionnain

Pagina 7: [“we won’t pay for your greed #2”](#)
by Alisdare Hickson

Pagina’s 8-11: [“Britain’s MOD sprayed blood red to highlight the UK’s complicity in Israel’s war crimes in Gaza #6”](#) by Alisdare Hickson

Pagina 12: [“sscs1014sbab10903”](#) by Santa Cruz Sentinel

Pagina 13: [“Fight Police Racism !”](#) by Alisdare Hickson

Pagina 14: [“Police - Paris, June 1992”](#) by Ian Abbott

Pagina 15: [“Politie overmeestert man”](#) by Shirley de Jong

Pagina 17: [“Palantir pavilion, World Economic Forum, Davos, Switzerland”](#) by Cory Doctorow

Pagina 18: [“manifest contre la «Loi Sécurité globale» à Paris le 28 novembre 2020 \(1\)”](#) by Jeanne Menjoulet

Pagina 21: [“Gendarmerie”](#) by Eddy Meulemans

Pagina 22: [“Spanish Police Colibrí”](#) by José Luis Celada Euba

Pagina 23: [“IMG_4601”](#) by Public Collectors

Pagina 27: [“Greater Manchester Police - BMW R1200RTs”](#) by Autumn

Pagina 30: [“Salt City 21”](#) by Office of Public Affairs

Pagina 34: [“manifest contre la «Loi Sécurité](#)

[globale» à Paris le 28 novembre 2020 \(2\)”](#)
by Jeanne Menjoulet

Pagina 37: [“VIDEO Überwachungsanlage”](#) by Christophe Stoll

Pagina 38: [“Torrevieja police vans ~ repeating patterns dailyshoot”](#) by Les Haines

Pagina 42: [“Protest against doublethink - a peace dove is a paraglider while genocide is self defence”](#) by Alisdare Hickson

Pagina 44: [“Brussels police \(2\)”](#) by Eoghan OLionnain

Pagina 46: [“#BlackLivesMatter protest in Stockholm, Sweden”](#) by Teemu Paananen

Pagina 48: [“IMG_0297”](#) by Steve Eason

Pagina 49: [“Police surveillance”](#) by York GreenParty

Pagina 53: [“_S9A0303”](#) ****by Steve Eason

Pagina 54: [“manifest contre la «Loi Sécurité globale» à Paris le 28 novembre 2020 \(3\)”](#)
by Jeanne Menjoulet

Pagina 56: [“Belgique - 21 juillet 2013 - Police - Politie - Polizei \(1\)”](#) by Antonio Ponte

Pagina 57: [“Belgique - 21 juillet 2013 - Police - Politie - Polizei \(2\)”](#) by Antonio Ponte

Pagina’s 58-61: [“Belgique - 21 juillet 2013 - Police - Politie - Polizei \(3\)”](#) by Antonio Ponte

Pagina 62: [“manifest contre la «Loi Sécurité globale» à Paris le 28 novembre 2020 \(4\)”](#)
Jeanne Menjoulet

Pagina 63: [“Fight Racism !”](#) by Alisdare Hickson

Eindnoten

1 Article 3(1), Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689#art_3

2 To give just one example, the definition in the Act is substantially different from the one included in the initial proposal. See: ‘Proposal for a Regulation laying down harmonised rules on artificial intelligence’, 21 April 2021, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>

3 Cabinet Office et al, ‘Ethics, Transparency and Accountability Framework for Automated Decision-Making’, 2021, <https://www.gov.uk/government/publications/ethics-transparency-and-accountability-framework-for-automated-decision-making/ethics-transparency-and-accountability-framework-for-automated-decision-making>

4 Cambridge Dictionary, ‘Machine learning’, <https://dictionary.cambridge.org/dictionary/english/machine-learning>

5 Amnesty International, ‘We Sense Trouble: automated discrimination and mass surveillance in predictive policing in the Netherlands’, 2020, <https://www.amnesty.org/en/wp-content/uploads/2021/05/EUR3529712020ENGLISH.pdf>

6 Links to all the reports are available at: <https://statewatch.org/predictivepolicing>

7 Lawrence Sherman, ‘The Cost-Effectiveness of Evidence-Based Policing’, 2010, https://eso.expertgrupp.se/wp-content/uploads/2010/07/2010_3-Sherman.pdf

8 Patrick Perrot, ‘L’analyse du risque criminel : l’émergence d’une nouvelle approche’, *Revue de l’Électricité*

et de l’Électronique, REE 2014-5 SEE, 2014, https://www.researchgate.net/publication/274071556_L'analyse_du_risque_criminel_l'emergence_d'une_nouvelle_approche.

9 EDRI, ‘Civil society calls on the EU to ban predictive AI systems in policing and criminal justice in the AI Act’, 2022, <https://edri.org/our-work/civil-society-calls-on-the-eu-to-ban-predictive-ai-systems-in-policing-and-criminal-justice-in-the-ai-act/>

10 Links to all the reports are available at: <https://statewatch.org/predictivepolicing>

11 European Union Agency for Fundamental Rights, ‘Second European Union Minorities and Discrimination Survey - Main results’, 2017, page 26, 29, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-eu-midis-ii-main-results_en.pdf

12 European Union Agency for Fundamental Rights, ‘Being Black in the EU — Experiences of people of African descent’, 2023, <https://fra.europa.eu/en/publication/2023/being-black-eu>

13 France 24, ‘Police violence: How can France tackle racial profiling without first addressing race?’, 9 July 2023, <https://www.france24.com/en/americas/20230709-france-s-police-dilemma-how-to-combat-racial-profiling-without-talking-about-race>

14 Amnesty International, ‘YOU NEVER KNOW WITH PEOPLE LIKE YOU’: POLICE POLICIES TO PREVENT ETHNIC PROFILING IN BELGIUM’, May 2018, https://www.amnesty-international.be/sites/default/files/bijlagen/ethnic_profiling_executive_summary_en.pdf

15 Rights International Spain and Open Society Justice Initiative, ‘Under Suspicion: The Impact of Discriminatory Policing in Spain’, 2019, Report: <https://>

www.justiceinitiative.org/uploads/21ac6560-639d-461c-a6b7-06822ad1c07e/under-suspicion-the-impact-of-discriminatory-policing-in-spain-20190924.pdf; Video:

<https://www.justiceinitiative.org/voices/under-suspicion-the-impact-of-discriminatory-policing-in-spain>

16 Arenas-García L and García-España E, 'Police stop and search in Spain: an overview of its use, impacts and challenges', March 2022, <https://indret.com/wp-content/uploads/2022/07/1715.pdf>

17 Bundeszentrale für Politische Bildung, 'Migration und Kriminalität – Erfahrungen und neuere Entwicklungen', 25 September 2020, <https://www.bpb.de/themen/innere-sicherheit/dossier-innere-sicherheit/301624/migration-und-kriminalitaet-erfahrungen-und-neuere-entwicklungen/#footnote-target-14>

18 Samantha Bielen, Peter Grajzl and Wim Marneffe, 'Blame Based on One's Name? Extralegal Disparities in Criminal Conviction and Sentencing', European Journal of Law and Economics, June 2021. DOI:[10.1007/s10657-020-09670-6](https://doi.org/10.1007/s10657-020-09670-6)

19 Fair Trials, 'Disparities and Discrimination in the European Union's Criminal Legal Systems', 2021 <https://www.fairtrials.org/app/uploads/2021/11/Disparities-and-Discrimination-in-the-European-Unions-Criminal-Legal-Systems.pdf>

20 Dieter Burssens, Carrol Tange, and Eric Maes, 'A la recherche de determinants du recours a la detention preventive et de sa duree', Institut National de Criminalistique et de Criminologie, 2015

21 Each One Teach One (EOTO), Citizens For Europe (CFE), 'Afrozensus 2020, Perspektiven, Anti-Schwarze Rassismuserfahrungen und Engagement Schwarzer, afrikanischer und afrodiasporischer Menschen in Deutschland', 2021, <https://afrozensus.de/reports/2020/Afrozensus-2020.pdf> (translated from German)

22 Germany report

23 Palantir, 'Palantir reports Q4 2024 Revenue Growth', 2025, <https://investors.palantir.com/news-details/2025/Palantir-Reports-Q4-2024-Revenue-Growth-of-36-YY-U.S.-Revenue-Growth-of-52-YY-Issues-FY-2025-Revenue-Guidance-of-31-YY-Growth-Eviscerating-Consensus-Estimates/>

24 With early funding stemming from In-Q-Tel, the venture capital arm of the CIA, Palantir's customers include: the CIA, NSA, FBI, ICE and army in the US, as well as the NHS in Britain.

25 See here for more information on the company's involvement in the Israeli occupation of Palestine: <https://dimse.info/briefcam/>

26 See here for information on the use of ClearView software by US police: <https://www.bbc.co.uk/news/technology-65057011>

27 Edicia, <https://www.edicia.fr/fr/>

28 Risk Terrain Modelling, <https://www.riskterrainmodeling.com/about.html>

29 Eurocop, <https://www.eurocop.com/>. El Salto (2021), 'El Estado policial español 2.0: tecnologías de empresas privadas para vigilar a los ciudadanos'. 4 February 2021. <https://www.elsaltodiario.com/tecnologia/estado-policial-espanol-2.0-empresas-privadas--vigilar-ciudadanos>

30 Securitas, <https://www.securitas.com/en/>

31 See here for more information on SopraSteria's contract with the EU for the 'Shared Biometric Matching System' (sBMS): [https://www.soprasteria.com/newsroom/press-releases/details/idemia-and-sopra-steria-chosen-by-eu-lisa-to-build-the-new-shared-biometric-matching-system-\(sbms\)-for-border-protection-of-the-schengen-area](https://www.soprasteria.com/newsroom/press-releases/details/idemia-and-sopra-steria-chosen-by-eu-lisa-to-build-the-new-shared-biometric-matching-system-(sbms)-for-border-protection-of-the-schengen-area)

32 James Bamford, 'How US Intelligence and an American Company Feed Israel's Killing Machine in Gaza', *The Nation*, 12 April 2024; 'Questions and Answers: Israeli Military's Use of Digital Tools in Gaza', *Human Rights Watch*, 10 September 2024, <https://www.hrw.org/news/2024/09/10/>

questions-and-answers-israeli-militarys-use-digital-tools-gaza

33 Forbes, 'Meet The Ex-NSA And Ex-Unit 8200 Spies Cashing In On Security Fears', 10 September 2014, <https://www.forbes.com/sites/kashmirhill/2014/09/10/meet-the-ex-nsa-and-ex-unit-8200-spies-cashing-in-on-security-fears/>

34 One definition of surveillance tech includes the following wide range of technologies: video surveillance (CCTV systems, IP cameras, video analytics software), big data (data analytics tools for surveillance data, predictive analytics for crime prevention), police body cameras (wearable cameras for law enforcement, recording and storage solutions), biometrics (fingerprint recognition technology, voice recognition systems), domestic drones (aerial surveillance drones for personal use, drones equipped with cameras and sensors), face recognition technology, Radio Frequency Identification tagging, and Stingray tracking devices (for mobile devices and intercepting cellular communications), see: The Business Research Company, 'Surveillance Technology Market Report', 2025. <https://www.thebusinessresearchcompany.com/report/surveillance-technology-global-market-report>. According to this definition, this report covers only predictive analytics for crime 'prediction', and AI video surveillance.

35 Ibid.

36 Article 5, AI Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689#art_5

37 <https://statewatch.org/predictivepolicing>

38 Chapter II, Article 5(d), Article 3(1), AI Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689#art_3

39 EU Commission, 'Commission publishes the Guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act', 4 February 2025, <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>

practices-defined-ai-act

40 Fair Trials, 'EU Parliament approves landmark AI law', 16 June 2023, <https://www.fairtrials.org/articles/news/eu-parliament-approves-landmark-ai-law/>

41 Investigate Europe 'France spearheads member state campaign to dilute European AI regulation', 22 January 2025 <https://www.investigate-europe.eu/posts/france-spearheads-member-state-campaign-dilute-european-artificial-intelligence-regulation>; TIME, 'Big Tech Is Already Lobbying to Water Down Europe's AI Rules', 21 April 2023, <https://time.com/6273694/ai-regulation-europe/>

42 European Digital Rights (EDRi), Access Now, Algorithm Watch, Bits of Freedom, European Disability Forum (EDF), European Not for Profit Law Center, Fair Trials, Panoptikon Foundation, and PICUM, 'Artificial Intelligence Act Amendments - Ensure meaningful transparency of AI systems for affected people', November 2021, https://panoptikon.org/sites/default/files/meaningful_transparency_for_people_affected_by_ai_art_52_aia_without_amendment_text.pdf

43 Article 86, AI Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689#art_86

44 Article 50, AI Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689#art_50

45 European Digital Rights (EDRi), Access Now, Algorithm Watch, Bits of Freedom, European Disability Forum (EDF), European Not for Profit Law Center, Fair Trials, Panoptikon Foundation, and PICUM 'Artificial Intelligence Act Amendments - Ensure rights and redress for people impacted by AI systems', November 2021, <https://edri.org/wp-content/uploads/2022/05/Rights-and-Redress-AIA-Amendments-for-online.pdf>

46 Article 85, AI Act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689#art_85

- 47 Germany report; Belgium report, France report. France in particular has weak freedom of information laws and performs poorly in the global 'freedom of information' index.
- 48 Spain report
- 49 Germany report
- 50 Braga, Anthony A., Barao, Lisa, 'Targeted Policing for Crime Reduction', Handbook on Crime and Deviance, Handbooks of Sociology and Social Research, Springer, 2019, https://doi.org/10.1007/978-3-030-20779-3_17
- 51 EU Commission, 'Commission publishes the Guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act', 4 February 2025, <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>
- 52 Germany report
- 53 Knobloch, Tobias, 'Vor die Lage kommen: Predictive Policing in Deutschland', Stiftung Neue Verantwortung, 29 August 2018, https://www.stiftung-nv.de/sites/default/files/predictive_policing.pdf
- 54 Germany report
- 55 Germany report
- 56 Camacho-Collados, M., & Liberatore, F, 'A decision support system for predictive police patrolling'. *Decision support systems*, 75, 25-37, 2015, <https://www.sciencedirect.com/science/article/abs/pii/S0167923615000834>
- 57 El Salto, 'El Estado policial español 2.0: tecnologías de empresas privadas para vigilar a los ciudadanos', 4 February 2021, **Error! Hyperlink reference not valid.**
- 58 France report
- 59 Belgium report
- 60 Orbit GIS, 'Zones de police', <https://www.orbitgis.com/fr/zone-de-police>
- 61 *The Markup*, 'Crime Prediction Software Promised to Be Free of Biases. New Data Shows It Perpetuates Them', 2021, <https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them>
- 62 Florian Gauthier, 'Prédire les vols de voitures ?', *Etalab blog*, 2018, <https://www.etalab.gouv.fr/predire-les-vols-de-voitures>
- 63 Abgeordnetenhaus Berlin, 'Bericht des Senats gemäß § 21 Absatz 4 Allgemeines Sicherheits- und Ordnungsgesetz (ASOG) für das Jahr 2021', 22 July 2022, <https://pardok.parlament-berlin.de/starweb/adis/citat/VT/19/DruckSachen/d19-0444.pdf> (translated from German)
- 64 France report
- 65 Germany report
- 66 Germany report, interview with Egbert, Simon, Postdoctoral Researcher 'The Future of Prediction', University of Bielefeld, 04 October 2023
- 67 Haco. 'Politiezone Westkust experimenteert met datasets in strijd tegen criminaliteit', *De Standaard*. 17 May 2016, https://standaard.be/cnt/dmf20160517_02292901
- 68 El Salto, 'El Estado policial español 2.0: tecnologías de empresas privadas para vigilar a los ciudadanos', 4 February 2021, **Error! Hyperlink reference not valid.**
- 69 Polizei Berlin, 'Kriminalitätsbelastete Orte', **Error! Hyperlink reference not valid.**
- 70 Orbit gis. 'Zones de police', <https://web.archive.org/web/20230930192819/https://www.orbitgis.com/fr/zone-de-police>; Orbit gis, 'Zones de police – Stratégie', https://www.orbitgis.com/fr/zone-de-police/zp_strategie
- 71 Haco. 'Politiezone Westkust experimenteert met datasets in strijd tegen criminaliteit'. *De Standaard*. 17 May 2016, https://standaard.be/cnt/dmf20160517_02292901
- 72 France report
- 73 Europol, 'Analysis and

prediction of crime’, <https://www.eurocop.com/sistemas-de-eurocop/analisis-y-prediccion-del-delito/>

74 Minister of Interior’s answer of 09/07/2020 to written question n°7-591. Belgian Senate, <https://senate.be/www/?Mlval=/Vragen/SVPrintNLFR&LEG=7&NR=591>

75 France report

76 France report

77 Quijano-Sánchez, L, ‘Applications of AI and Data Science in Policing: 7 years of collaborations with the Spanish Police’. Lara Quijano-Sánchez, Ph.D by the Politechnic School of the Universidad Autónoma de Madrid. 25 January 2022, <https://www.youtube.com/watch?v=z8uBNNPtUmE>; Liberatore, F., Camacho-Collados, M., & Quijano-Sánchez, L, ‘Towards social fairness in smart policing: Leveraging territorial, racial, and workload fairness in the police districting problem’, *Socio-Economic Planning Sciences*, 87, 101556, 2023, <https://www.sciencedirect.com/science/article/pii/S0038012123000563#sec5>

78 Ibid.

79 Article 10, Law Enforcement Directive, <https://eur-lex.europa.eu/eli/dir/2016/680/oj>

80 Recital 38 and Article 11, Law Enforcement Directive, <https://eur-lex.europa.eu/eli/dir/2016/680/oj>

81 German report, France report, Belgium report.

82 Polizei Berlin, ‘Kriminalitätsbelastete Orte’, <https://www.berlin.de/polizei/polizeimeldungen/fakten-hintergruende/artikel.1078268.php>, (translated from German)

83 France report

84 Lina Schmid, ‘Grundrechte in Gefahr(engebieten). Verfassungsrechtliche Beurteilung der polizeilichen Praxis “kriminilitätsbelasteter Orte”, 2023, in *Mythos Generalverdacht. Wie mit dem Mythos Clankriminalität Politik gemacht wird*, Nautilus

Flugschrift, p.167, translated from German.

85 Süddeutsche Zeitung, ‘Unbeteiligte geraten ins Kontrollraster’, 12 Sept 2014, <https://www.sueddeutsche.de/wirtschaft/ueberwachung-mit-predictive-policing-unbeteiligte-geraten-ins-kontrollraster-1.2115126> (translated from German)

86 Lina Schmid, ‘Grundrechte in Gefahr(engebieten). Verfassungsrechtliche Beurteilung der polizeilichen Praxis “kriminilitätsbelasteter Orte”, 2023, in *Mythos Generalverdacht. Wie mit dem Mythos Clankriminalität Politik gemacht wird*, Nautilus Flugschrift, p.167, translated from German

87 Wrangelkiez United, ‘Perspektiven: Realitäten von Geflüchteten’, Video, <https://wrangelkiezunited.noblogs.org/home/>, translated from German

88 Ibid

89 George L. Kelling and James Q. Wilson, *The Atlantic*, ‘Broken Windows: The Police and Neighbourhood Safety’, 1982, <https://www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/>

90 Donna Ladd, ‘Inside William Bratton’s NYPD: broken windows policing is here to stay’, *The Guardian*, 2015, <https://www.theguardian.com/us-news/2015/jun/08/inside-william-bratton-nypd-broken-windows>

91 ‘Northeastern University researchers find little evidence for ‘broken windows theory,’ say neighborhood disorder doesn’t cause crime’, *Northeastern Global News*, 15 May 2019, <https://news.northeastern.edu/2019/05/15/northeastern-university-researchers-find-little-evidence-for-broken-windows-theory-say-neighborhood-disorder-doesnt-cause-crime/>

92 Amnesty International UK, ‘Automated Racism: How police data and algorithms code discrimination into policing’, February 2025, <https://www.amnesty.org.uk/files/2025-02/Automated%20Racism%20Report%20-%20Amnesty%20International%20>

93 Risk Terrain Modelling, ‘Spatial dynamics of crime’, <https://www.riskterrainmodeling.com/overview.html>

94 Ibid.

95 Following its closure in 2020, part of the *Observatoire*’s activities have been transferred to the French Ministry of the Interior’s *Service Statistique Ministériel de la Sécurité Intérieure* (SSMSI, part of the *Institut des hautes études du ministère de l’Intérieur* or IHEMI, created in September 2020).

96 Camille Gosselin, ‘La police prédictive : enjeux soulevés par l’usage des algorithmes prédictifs en matière de sécurité publique’, Paris: IAU Île-de-France, 2019, https://www.institutparisregion.fr/fileadmin/NewEtudes/Etude_1797/Etude_Police_Predictive_V5.pdf

97 Belgium report

98 Sûreté Globale website, <https://web.archive.org/web/20230610153444/https://www.sureteglobale.org>

99 France report

100 Risk Terrain Modelling, ‘Spatial dynamics of crime’, <https://www.riskterrainmodeling.com/overview.html>

101 Thibault Sardier, ‘Cartographie criminelle : surveiller et prédire’, *lemonde.fr*, 5 January 2018, https://www.lemonde.fr/idees/article/2018/01/05/cartographie-criminelle-surveiller-et-predire_5237723_3232.html

102 Anneleen Rummens & Wim Hardyns, ‘Comparison of near-Repeat, Machine Learning and Risk Terrain Modeling for Making Spatiotemporal Predictions of Crime’. *Applied Spatial Analysis and Policy*, 2021, Vol. 13, no. 4, pp. 1035–1053. DOI: 10.1007/s12061-020-09339-2

103 International terrorism database, <https://www.start.umd.edu/gtd/access/>. It shows that France only has 20 entries from 2016 to 2019, which leaves one wondering about the relevance

of this dataset.

104 France report

105 France report

106 Amnesty International UK, ‘Automated Racism: How police data and algorithms code discrimination into policing’, February 2025, <https://www.amnesty.org.uk/files/2025-02/Automated%20Racism%20Report%20-%20Amnesty%20International%20UK%20-%202025.pdf>

107 Amnesty International UK, ‘Automated Racism: How police data and algorithms code discrimination into policing’, February 2025, <https://www.amnesty.org.uk/files/2025-02/Automated%20Racism%20Report%20-%20Amnesty%20International%20UK%20-%202025.pdf> p.69

108 Ibid.

109 Ibid.

110 Fair Trials, ‘Automating Injustice: The Use of Artificial Intelligence & Automated Decision-Making Systems in Criminal Justice in Europe’, 09 September 2021, **Error! Hyperlink reference not valid.;**

111 Gatti, Carlo, ‘Monitoring the monitors: a demystifying gaze at algorithmic prophecies in policing’, 10 November 2022, *Justice, Power and Resistance*, 5(3), 227-248, <https://doi.org/10.1332/UBQA2752>

112 AlgorithmWatch, ‘The Rise and Fall of a Predictive Policing Pioneer’, 7 November 2024, <https://algorithmwatch.org/en/predictive-policing-pioneer-keycrime/>; Wired, ‘Perché la più avanzata startup italiana di polizia predittiva è sull’orlo del baratro’, 31 January 2024, <https://www.wired.it/article/polizia-predittiva-keycrime-startup-ai-act/>

113 Gatti, Carlo, ‘Monitoring the monitors: a demystifying gaze at algorithmic prophecies in policing’, 10 November 2022, *Justice, Power and Resistance*, 5(3), 227-248, <https://doi.org/10.1332/UBQA2752>

- 114 *Ibid.*
- 115 AlgorithmWatch, 'Automating Society Report 2020 — Swiss Edition', January 2021, <https://automatingsociety.algorithmwatch.org/report2020/switzerland/>
- 116 Belgium report
- 117 Williams, P, 'Criminalising the Other: challenging the race-gang nexus', *Race & Class*, 2014, 6(3), 18-35. <https://doi.org/10.1177/0306396814556221>
- 118 Belgium report
- 119 The terms 'terrorist', 'terrorism', 'Islamist', 'extremism', 'extremist' and 'radicalisation' are ill-defined, imprecise and easily misused. As they routinely appear in laws, policies, government statements and academic research, however, they are used in this report for ease of reference. This does not imply that their use or definition by government institutions is endorsed. Per Amnesty UK, 'This Is The Thought Police: The Prevent duty and its chilling effect on human rights', November 2023, <https://www.amnesty.org.uk/files/2023-11/Amnesty%20UK%20Prevent%20report%20%281%29.pdf>
- 120 Belgium report
- 121 'EU: Definition of "potential terrorists" opens door to broad information-sharing', *Statewatch*, 2 October 2024, <https://www.statewatch.org/news/2024/october/eu-definition-of-potential-terrorists-opens-door-to-broad-information-sharing/>
- 122 Bundeskriminalamt, 'RADAR (Regelbasierte Analyse potentiell destruktiver Täter zur Einschätzung des akuten Risikos)', https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/PMK/Radar/radar_node.html
- 123 Eticas Research, 'The external audit of the VioGen system', 8 March 2022; Bayona, J. Z. (2014). *Violencia contra la mujer: marco histórico evolutivo y predicción del nivel de riesgo* (Doctoral dissertation, Universidad Autónoma de Madrid), <https://dialnet.unirioja.es/servlet/tesis?codigo=43479>
- 124 Quijano-Sánchez, L., Liberatore, F., Camacho-Collados, J., & Camacho-Collados, M, 'Applying automatic text-based detection of deceptive language to police reports: Extracting behavioral patterns from a multi-step classification model to understand how we lie to the police', *Knowledge-Based Systems*, 2018, 149, 155-168, <https://www.sciencedirect.com/science/article/abs/pii/S095070511830128X?via%3DiHub>; Nature, 'Police use a computer to expose false testimony', 30 May 2018, <https://www.nature.com/articles/d41586-018-05285-9>
- 125 Civio, 'Spanish National Police stop using Veripol, its star AI for detecting false reports', 25 March 2025 <https://civio.es/transparencia/2025/03/25/national-police-stop-using-veripol-its-star-ai-for-detecting-false-reports/>
- 126 Germany report; 'PNR for all: UN Security Council mandates worldwide air travel surveillance and profiling, biometric collection, terrorist watchlists', *Statewatch*, 8 January 2018, <https://www.statewatch.org/news/2018/january/un-pnr-for-all-un-security-council-mandates-worldwide-air-travel-surveillance-and-profiling-biometric-collection-terrorist-watchlists/>
- 127 Germany report.
- 128 Tony Bunyan, 'EU: The surveillance of travel where everyone is a suspect', *Statewatch*, August 2008, <https://www.statewatch.org/media/documents/analyses/no-70-eu-travel-surveillance.pdf>
- 129 European Commission, 'ProtectEU: a European Internal Security Strategy', COM(2025) 148 final, 1 April 2025, https://home-affairs.ec.europa.eu/document/download/48218e1a-9e03-4be1-b19c-d04c323c1117_en?filename=ProtectEU-European-Internal-Security-Strategy_en.pdf
- 130 Senate, 'Orden de servicio 3/2018', February 2018, <https://www.senado.es/web/expedientappendixblobervlet?legis=12&id1=119003&id2=1>

131 Andrés Pueyo, A., Arbach Lucioni, K., & Redondo, S., 'The RisCanvi: a new tool for assessing risk for violence in prison and recidivism', *Handbook of recidivism risk/needs assessment tools*, 2018, 255-268, <https://onlinelibrary.wiley.com/doi/abs/10.1002/9781c119184256.ch13>; AlgorithmWatch (2021), 'In Catalonia, the RisCanvi algorithm helps decide whether inmates are paroled', 25 May 2021, <https://algorithmwatch.org/en/riscanvi/>

132 Justizportal Nordrhein-Westfalen, § 25a HSOG Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) Landesrecht Hessen, https://www.lexsoft.de/cgi-bin/lexsoft/justizportal_nrw.cgi?xid=169564,130; Gesellschaft für Freiheitsrechte, 'NRW Assembly Act: Threat to freedom of assembly and civil-society', <https://freiheitsrechte.org/en/themen/demokratie/vb-versammlungsrecht-nrw>

133 Germany report

134 Harry Davies, Bethan McKernan, Dan Sabbagh. 'The Gospel': how Israel uses AI to select bombing targets in Gaza', *The Guardian*, 1 December 2023, www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets

135 Rights International Spain and Open Society Justice Initiative, 'Under Suspicion: The Impact of Discriminatory Policing in Spain', 2019. Report: <https://www.justiceinitiative.org/uploads/21ac6560-639d-461c-a6b7-06822ad1c07e/under-suspicion-the-impact-of-discriminatory-policing-in-spain-20190924.pdf>; Video:

<https://www.justiceinitiative.org/voices/under-suspicion-the-impact-of-discriminatory-policing-in-spain>; Arenas-García L and García-España E, 'Police stop and search in Spain: an overview of its use, impacts and challenges', March 2022, <https://indret.com/wp-content/uploads/2022/07/1715.pdf>

136 Bundeszentrale für Politische Bildung, 'Migration und Kriminalität – Erfahrungen und neuere Entwicklungen', 25 September 2020, <https://www.bpb.de/themen/innere-sicherheit/>

[dossier-innere-sicherheit/301624/migration-und-kriminalitaet-erfahrungen-und-neuere-entwicklungen/#footnote-target-14](https://www.bpb.de/themen/innere-sicherheit/301624/migration-und-kriminalitaet-erfahrungen-und-neuere-entwicklungen/#footnote-target-14)

137 Jérémie Vervoort, 'I-Police ou l'art de prédire la discrimination', Travail de fin d'études, Brussels: Université libre de Bruxelles, 2021

138 CERD, 'Concluding observations on the sixteenth to nineteenth periodic reports of Belgium', *United Nations Committee on the Elimination of Racial Discrimination*. cerd/c/bel/co/16-19, 2014, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CERD%2FC%2FBEL%2FCO%2F16-19

139 Germany report

140 Welt, 'So funktioniert das Radar für radikale Islamisten', 12 June 2017, <https://www.welt.de/politik/deutschland/plus165451390/So-funktioniert-das-Radar-fuer-radikale-Islamisten.html>

141 Germany report

142 Germany report

143 Quijano-Sánchez, L., Liberatore, F., Camacho-Collados, J., & Camacho-Collados, M. (2018), 'Applying automatic text-based detection of deceptive language to police reports: Extracting behavioral patterns from a multi-step classification model to understand how we lie to the police', *Knowledge-Based Systems*, 149, 155-168, <https://www.sciencedirect.com/science/article/abs/pii/S095070511830128X?via%3Dihub>

144 Eticas Research, 'The external audit of the VioGen system', 8 March 2022.

145 Eticas Research, 'The external audit of the VioGen system', 8 March 2022.

146 Tagesschau, 'Immer mehr rechte Gefährder', 26 June 2022, <https://www.tagesschau.de/inland/rechte-gefaehrder-103.html>

147 Belgium report

148 Germany report

- 149 Germany report
- 150 Germany report
- 151 Secretary of State for Security, 'Instruction nº 7/2016', 8 July 2016, https://violenciagenero.igualdad.gob.es/wp-content/uploads/Instruccion7_2016.pdf
- 152 Bayona, J. Z, *Violencia contra la mujer: marco histórico evolutivo y predicción del nivel de riesgo* (Doctoral dissertation, Universidad Autónoma de Madrid), 2014, <https://dialnet.unirioja.es/servlet/tesis?codigo=43479>
- 153 Kanzlei Redecker Sellner Dahs, 'Stellungnahme an das Verwaltungsgericht Wiesbaden', 09 September 2021
- 154 Secretary General of Penitentiary Institutions, Ministry of Interior, 'Construcción y validación de una herramienta de clasificación y de valoración del riesgo de radicalismo violento en el ámbito penitenciario', 2021 https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/instituciones-penitenciarias/Construccion-y-validacion-de-una-herramienta-de-clasificacion-y-de-valoracion-del-riesgo-de-radicalismo-violento-en-el-ambito-penitenciario_126210405.pdf
- 155 *Ibid*
- 156 Karimi-Haghighi, M., & Castillo, C., 'Efficiency and fairness in recurring data-driven risk assessments of violent recidivism', In *Proceedings of the 36th Annual ACM Symposium on Applied Computing* (pp. 994-1002), March 2021 https://chato.cl/papers/karimi_haghighi_castillo_2021_efficiency_fairness_temporal_recurring.pdf
- 157 Ministry of Interior, 'Statistical data Viogen', September 2023, <https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/violencia-contra-la-mujer/estadisticas/2023/Estadistica-Septiembre-2023.pdf>
- 158 Germany report
- 159 Germany report
- 160 Germany report
- 161 MDR, 'Sachsen-Anhalt will Polizei-Gewahrsam bei Terrorverdacht verlängern', 17 December 2023 <https://www.mdr.de/nachrichten/sachsen-anhalt/polizei-gewahrsam-gesetz-aenderung-terrorverdacht-100.html>
- 162 *Ibid*
- 163 Tagesspiegel, 'Neue Plätze für 40 Straftäter – im Abschiebeknast', 31 January 2024, <https://www.tagesspiegel.de/berlin/losung-fur-berliner-massregelvollzug-neue-platze-fur-40-straftater-im-abschiebeknast-11137660.html>
- 164 Tagesschau, 'Warum die Abschiebepläne kaum einzuhalten sind', 04 October 2022, <https://www.tagesschau.de/investigativ/ndr-wdr/koalition-abschiebungen-gefaehrder-101.htm>
- 165 Deutscher Bundestag, 'Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökyak Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE, Drucksache 19/5202, Personenpotentiale islamistischer „Gefährder“', 9 November 2018, <https://dserver.bundestag.de/btd/19/056/1905648.pdf> (translated from German)
- 166 Amnesty International UK, 'Automated Racism: How police data and algorithms code discrimination into policing', February 2025 <https://www.amnesty.org.uk/files/2025-02/Automated%20Racism%20Report%20-%20Amnesty%20International%20UK%20-%202025.pdf?VersionId=JqCcTODw37yAXyINmAY6uAzrKEWucFF7>
- 167 The Conversation, 'A black box' AI system has been influencing criminal justice decisions for over two decades — it's time to open it up', 26 July 2023, <https://theconversation.com/a-black-box-ai-system-has-been-influencing-criminal-justice-decisions-for-over-two-decades-its-time-to-open-it-up-200594>; 'UK: Over 1,300 people profiled daily by Ministry of Justice AI system to 'predict' re-offending risk', *Statewatch*, 9 April

2025, <https://www.statewatch.org/news/2025/april/uk-over-1-300-people-profiled-daily-by-ministry-of-justice-ai-system-to-predict-re-offending-risk/>

168 Fair Trials, 'Automating Injustice: The Use of Artificial Intelligence & Automated Decision-Making Systems in Criminal Justice in Europe', 09 September 2021, **Error! Hyperlink reference not valid.**

169 Ibid.

170 Fair Trials, 'My sons were profiled by a racist predictive policing system — the AI Act must prohibit these systems', 28 September 2022, <https://medium.com/@FairTrials/my-sons-were-profiled-by-a-racist-predictive-policing-system-the-ai-act-must-prohibit-these-b2ea66a9a763>

171 Fair Trials, 'Automating Injustice: The Use of Artificial Intelligence & Automated Decision-Making Systems in Criminal Justice in Europe', 9 September 2021, <https://www.fairtrials.org/articles/publications/automating-injustice/>; Gatti, Carlo, 'Monitoring the monitors: a demystifying gaze at algorithmic prophecies in policing', 10 November 2022, *Justice, Power and Resistance*, 5(3), 227-248, <https://doi.org/10.1332/UBQA2752>

172 La Quadrature du Net, 'Non à la vidéosurveillance algorithmique, refusons l'article 7 de la loi olympique!', 18 January 2023, <https://www.laquadrature.net/2023/01/18/non-a-la-videosurveillance-algorithmique-refusons-l'article-7-de-la-loi-olympique/>

173 See the 'Law Enforcement and Corrections' webpage on the ISS website: <https://issivs.com/served-verticals/law-enforcement-and-corrections/>

174 El País, 'Marbella, el mayor laboratorio de videovigilancia de España', 22 November 2019, https://elpais.com/tecnologia/2019/11/21/actualidad/1574348695_231540.html

175 La VanGuardia, 'Madrid has 83 cameras on the streets with artificial intelligence Surveillance', 9 January

2025 <https://www.lavanguardia.com/mediterranean/20250109/10268393/madrid-83-cameras-street-artificial-intelligence-surveillance-install-mayor-martinez-almeida-spain-city-council-police-technology.html>

176 Nicolas Bocquet, 'The Brussels Smart City: how "intelligence" can be synonymous with video surveillance'. *Brussels Studies*, 2021, journals.openedition.org/brussels/5678

177 La Quadrature du Net, 'France becomes the first European country to legalize biometric surveillance' 29 March 2023, <https://www.laquadrature.net/en/2023/03/29/france-becomes-the-first-european-country-to-legalize-biometric-surveillance/>

178 Jacobin, 'Emmanuel Macron Is Using the 2024 Olympics to Make France a Surveillance State', 21 March 2023 <https://jacobin.com/2023/03/emmanuel-macron-2024-olympics-surveillance-state-ai-biometric-system>

179 Jacobin, 'France Wants to Make Olympics-Style Surveillance Permanent', 23 October 2024 <https://jacobin.com/2024/10/france-olympics-surveillance-ai-policing>

180 ID Tech Editorial Team, 'French Court Rules Briefcam's AI Surveillance System Unlawful', 31 January 2025, <https://idtechwire.com/french-court-rules-briefcams-ai-surveillance-system-illegal/>

181 Ibid.

182 Ministerium der Justiz des Landes Nordrhein-Westfalen, 'Bericht zum TOP „Todesfälle und Suizide im Strafvollzug. 84. Sitzung des Rechtsausschusses des Landtags Nordrhein-Westfalen am 27.10.2021', 25 October 2021. www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV17-5871.pdf

183 Ibid.

184 Germany report

185 Niedersächsischer Landtag, 'Antrag, Einsatz künstlicher Intelligenz zur Suizidprävention und Verbesserung

- der Sicherheit in niedersächsischen Justizvollzugsanstalten', Drucksache 18/8729, 09 March 2021, https://www.landtag-niedersachsen.de/Drucksachen/Drucksachen_18_10000/08501-09000/18-08729.pdf, translated from German
- 186 Landesbeauftragte für den Datenschutz Niedersachsen, '27. Tätigkeitsbericht 2021', 2021, <https://www.lfd.niedersachsen.de/startseite/infothek/tatigkeitsberichte/2021/barbara-thiel-stellt-tatigkeitsbericht-2021-vor-212174.html>, translated from German
- 187 Germany report
- 188 Barrett, L. F. et al., 'Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements', *Psychological Science in the Public Interest*, 20(1), 1-68, 2019. <https://journals.sagepub.com/doi/10.1177/1529100619832930>
- 189 Rhue, Lauren, 'Racial Influence on Automated Perceptions of Emotions', 9 November 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765
- 190 Article 19, 'Emotional Entanglement: China's emotion recognition market and its implications for human rights', 19 November 2020
- 191 Germany report
- 192 AlgorithmWatch, 'Spanish Inmates Not to Be Automatically Monitored in Fear of AI Act', 28 March 2024 <https://algorithmwatch.org/en/spanish-inmates-not-monitored-in-fear-of-ai-act/>
- 193 Belgium report
- 194 Statewatch, 'France: Green light for police surveillance of political opinions, trade union membership and religious beliefs', 13 January 2021, <https://www.statewatch.org/news/2021/january/france-green-light-for-police-surveillance-of-political-opinions-trade-union-membership-and-religious-beliefs/>
- 195 France report
- 196 France report
- 197 Camille Gosselin, 'La police prédictive : enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique', (Paris: IAU Île-de-France, 2019), https://www.institutparisregion.fr/fileadmin/NewEtudes/Etude_1797/Etude_Police_Predictive_V5.pdf
- 198 Ibid
- 199 Didier Paris and Pierre Morel-À-L'Huissier, 'Rapport sur les fichiers mis à la disposition des forces de sécurité', Commission des Lois constitutionnelles, de la législation et de l'administration générale de la République (Paris: Assemblée Nationale, Commission des Lois), October 2018, <http://www.assemblee-nationale.fr/15/rap-info/i1335.asp>
- 200 La Quadrature du Net, 'La reconnaissance faciale des manifestants est déjà autorisée', 18 November 2019, <https://www.laquadrature.net/2019/11/18/la-reconnaissance-faciale-des-manifestants-est-deja-autorisee/>
- 201 France report
- 202 Statewatch/Platform for International Cooperation on Undocumented Migrants, 'Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status', 18 November 2019, <https://www.statewatch.org/publications/reports-and-books/data-protection-immigration-enforcement-and-fundamental-rights-what-the-eu-s-regulations-on-interoperability-mean-for-people-with-irregular-status/>
- 203 France report
- 204 Sainz de la Maza Quintanal, E, "'Ultima ratio": el proceso de expulsión de inmigrantes en situación irregular en España', 2015, <https://docta.ucm.es/entities/publication/769b2a6c-8db4-4e2f-8fbe-623cb7c9ce6c>
- 205 Valdivia, A., & Tazzioli, M, 'Datafication Genealogies beyond Algorithmic Fairness: Making Up Racialised Subjects', in *Proceedings of the 2023 ACM Conference on Fairness, Accountability,*

and Transparency (pp. 840-850), June 2023,
<https://doi.org/10.1145/3593013.3594047>

206 Belgium report, Germany report, France report

207 Matthias Monroy, 'Suspicion files: German police databases on political activists', *Statewatch*, 10 April 2018, <https://www.statewatch.org/analyses/2018/suspicion-files-german-police-databases-on-political-activists/>

208 Belgium report

209 Belgium report

210 Belgium report

211 Rights International Spain and Open Society Justice Initiative, 'Under Suspicion: The Impact of Discriminatory Policing in Spain', 2019. Report: <https://www.justiceinitiative.org/uploads/21ac6560-639d-461c-a6b7-06822ad1c07e/under-suspicion-the-impact-of-discriminatory-policing-in-spain-20190924.pdf>; Video:

<https://www.justiceinitiative.org/voices/under-suspicion-the-impact-of-discriminatory-policing-in-spain>

212 Belgium report, France report

213 Belgium report

214 Belgium report, France report

215 Reuters, 'In a U.S. first, California city set to ban predictive policing', 19 June 2020, <https://www.reuters.com/article/us-usa-police-tech-trfn/in-a-us-first-california-city-set-to-ban-predictive-policing-idUSKBN23031A/>

216 EDRI, 'Civil society calls on the EU to ban predictive AI systems in policing and criminal justice in the AI Act', 1 March 2022, <https://edri.org/our-work/civil-society-calls-on-the-eu-to-ban-predictive-ai-systems-in-policing-and-criminal-justice-in-the-ai-act/>

217 <https://technopolice.fr/>

218 <https://technopolice.be/>

219 <https://www.openrightsgroup.org/campaign/safety-not-surveillance/>

220 <https://stoplapdspying.org/>