



NEUE TECHNIK ALTE UNGE- RECHTIGKEIT

DATENBASIERTE DISKRIMINIERUNG UND
KRIMINALISIERUNG BEI POLIZEI UND IN
GEFÄNGNISSEN IN EUROPA

GESCHRIEBEN VON:

Griff Ferris

Sofia Lyall

FINANZIERT VON:

European
Artificial Intelligence
& Society Fund

Publikations- information- en

Autor*innen: Griff Ferris, Sofia Lyall

Herausgeber: Chris Jones

Design: McKensie Marie

Dieser Bericht wurde von der European AI & Society Foundation gefördert.

Veröffentlicht von Statewatch, Juni 2025.

Om Statewatch

Statewatch produziert und fördert kritische Forschung, Politikanalysen und investigativen Journalismus, um Debatten, Bewegungen und Kampagnen für Bürger*innen und Menschenrechte sowie demokratische Standards zu unterstützen. Wir sind seit 1991 in London tätig.

statewatch.org

(+44) (0) 203 393 8366

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

Uns unter- stützen

U kan ons werk steunen via giften:



Inschrijven op onze nieuwsbrief:

— [Anmelden](#)

Registrierte britische

Wohltätigkeitsorganisationsnummer:
1154784

Registrierte britische

Unternehmensnummer: 08480724

Registrierter Unternehmensname: The
Libertarian Research & Education Trust

Registrierter Sitz: 88 Fleet Street,
London EC4Y 1DH, UK.

Inhalt

Danksagung	4
Definitionen	5
Zusammenfassung	7
Einleitung	12
Systeme zur standortbezogenen Vorhersage	23
Personenbezogene Systeme zur Vorhersage und zum Profiling	38
KI-Videoüberwachungs-systeme	49
Datenbanken	53
Fazit	57
Bildnachweise	64
Endnoten	65

Danksagung

Diese Arbeit wurde durch Forschende und Partnerorganisationen in Belgien, Frankreich, Deutschland und Spanien ermöglicht:

- Belgien: Corentin Debailleul, Technopolice Belgien und Ligue des droits humains;
- Frankreich: Edlira Nano und Félix Tréguer, La Quadrature du Net, mit Unterstützung von Mitgliedern der Arbeitsgruppe Technopolice Frankreich von La Quadrature du Net;
- Deutschland: Sonja Peteranderl, AlgorithmWatch;
- Spanien: Naiara Bellio, mit ihren Mitarbeitenden Ana Valdivia und Javier Sánchez Monedero, AlgoRace.

Wir danken allen Personen und Gruppen, die an Interviews teilgenommen oder auf andere Weise Informationen, Erfahrungen oder Fachwissen zur Verfügung gestellt haben.

Wir möchten uns auch für die Arbeit von Personen und Organisationen bedanken, die sich gegen Rassismus und Diskriminierung in Polizei- und Strafrechtssystemen einsetzen, von denen diese neuen Technologien nur die jüngste Entwicklung darstellen.

Definitionen

Künstliche Intelligenz

Die Verordnung zur künstlichen Intelligenz der Europäischen Union definiert ein KI-System wie folgt:

„...ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können.“¹

In diesem Bericht wird diese Definition verwendet, obwohl es viele Möglichkeiten gibt, KI und KI-Systeme zu definieren.² Es ist wichtig zu beachten, dass die meisten datenbasierten, algorithmischen und automatisierten Systeme, die von Polizei- und Strafverfolgungsbehörden in Europa eingesetzt werden, keine künstliche Intelligenz nutzen. Manche dieser Systeme nutzen maschinelles Lernen (siehe unten), ein Teilgebiet der KI. Die Mehrheit dieser Systeme verwendet jedoch klassische statistische Methoden und kann als automatisiertes System zur Entscheidungsfindung bezeichnet werden (siehe unten).

Automatisiertes System zur Entscheidungsfindung

Das britische Amt für KI definiert automatisierte Systeme zur Entscheidungsfindung als solche, die „ausschließlich automatisierte Entscheidungen (ohne menschliches Urteilsvermögen)“ sowie „automatisierte unterstützte Entscheidungsfindung (Unterstützung des menschlichen Urteilsvermögens)“ verwenden.³

Maschinelles Lernen

Der Cambridge Dictionary definiert maschinelles Lernen als „den Prozess, bei dem Computer ihre Fähigkeit zur Aufgabenerfüllung durch die Analyse neuer Daten verbessern, ohne dass ein Mensch Anweisungen in Form eines Programms geben muss bzw. als das Studium der Entwicklung und Nutzung von Computersystemen, die dies leisten können“.⁴

Predictive Policing:

Es gibt zwei Hauptarten von Predictive Policing, der „vorausschauenden Polizeiarbeit“: standort- oder ortsbezogen und personenbezogen. Amnesty International definiert Systeme zum Predictive Policing wie folgt:

„...Computerprogramme, die Daten und algorithmische Modelle nutzen, um das Risiko einer Straftat zu bewerten. Systeme zum Predictive Policing berechnen Risikobewertungen, die die Wahrscheinlichkeit widerspiegeln, dass eine Person oder Gruppe Opfer oder Täter ist oder sein wird (personenbezogenes Predictive Policing) oder dass ein bestimmter Ort ein zukünftiger Tatort sein wird (ortsbezogenes Predictive Policing). Auf Grundlage dieser computergenerierten Risikobewertungen ergreift die Polizei Maßnahmen zur Verhinderung oder Aufdeckung der vorhergesagten Straftaten, indem sie ihre Polizeiarbeit auf Orte, Personen oder Gruppen mit hohem Risiko richtet.“⁴⁵





Zusammenfassung

Polizei und Strafjustizbehörden in ganz Europa nutzen zunehmend datenbasierte Systeme und Instrumente, um Tatorte vorherzusagen, Profile von Personen als Kriminelle zu erstellen und das Risiko zukünftiger Straftaten einzuschätzen.

Diese sogenannten „Vorhersagen“, Profile und Risikobewertungen beeinflussen polizeiliche Entscheidungen, Maßnahmen und Interventionen. Dazu gehören Überwachung und Beobachtung, Befragungen, Personenkontrollen, Identitätsprüfungen, Arbeitsverbote, Hausdurchsuchungen, Geldstrafen, Gewaltanwendung, Inhaftierung, Festnahme und Abschiebung.

Diese datenbasierten Systeme und Entscheidungen beeinflussen auch Entscheidungen im gesamten Strafrechtssystem: von der Haft und Untersuchungshaft bis hin zu Strafverfolgung, Verurteilung und Bewährung.

Außerhalb des Strafrechtssystems können automatisierte Entscheidungen auch andere Formen der Bestrafung beeinflussen oder zu diesen führen. Beispielsweise können sie die Verweigerung oder Einschränkung des Zugangs zu wichtigen öffentlichen Dienstleistungen wie Sozialleistungen oder Wohnraum begründen.

In diesem Bericht wird Originalforschung zu automatisierten Entscheidungsfindungssystemen und Datenbanken, die in der Polizeiarbeit und in Strafrechtssystemen in vier Ländern eingesetzt

werden, zusammengefasst: Belgien, Frankreich, Deutschland und Spanien. Der Bericht basiert auf umfassenden Untersuchungen von Partnerorganisationen in diesen Ländern.⁶ Er geht auf Folgendes ein:

- wie diese datenbasierten Systeme zur Kriminalitätsvorhersage entwickelt werden;
- wie sie von Strafverfolgungs- und Strafjustizbehörden genutzt werden;
- die von den Systemen erzeugten Ergebnisse;
- wie diese Ergebnisse genutzt werden und Entscheidungen beeinflussen und welche Auswirkungen diese auf Personen, Gruppen und Gemeinschaften haben.

Es wird auch untersucht, wie marginalisierte Gruppen und Gemeinschaften überproportional von diesen Systemen ins Visier genommen werden und betroffen sind, darunter schwarze und rassifizierte Personen und Gemeinschaften, Opfer geschlechtsspezifischer Gewalt, Migrant*innen und Personen aus der Arbeiterklasse und sozioökonomisch benachteiligten Schichten und Gebieten sowie Personen mit psychischen Erkrankungen.

Die meisten dieser Systeme nutzen historische Daten, beispielsweise von der Polizei oder dem Strafjustizsystem. Dies spiegelt historische und bestehende Vorurteile innerhalb dieser Institutionen und in der Gesellschaft wider. Dies führt zu einer übermäßigen Polizeipräsenz und Kriminalisierung marginalisierter Gemeinschaften, insbesondere rassifizierter Gruppen, Migrant*innen und Personen aus einkommensschwachen Vierteln.

Der Einsatz dieser Systeme in der Polizeiarbeit und im Strafrechtssystem hat erhebliche Auswirkungen auf die Rechte des Einzelnen, darunter das Recht auf ein faires Verfahren, Privatsphäre und Diskriminierungsfreiheit.

Systeme zum standortbezogenen Predictive Policing

In ganz Europa entwickeln und implementieren Polizeibehörden standortbezogene Methoden des Predictive Policing. Diese algorithmischen Systeme sollen „vorhersagen“, wo und wann eine



Straftat begangen wird. Dies ermöglicht es der Polizei, Ressourcen gezielt an diesen Orten einzusetzen. Geografische Systeme zur Kriminalitätsvorhersage werden oder wurden in allen vier untersuchten Ländern eingesetzt: in Belgien, Frankreich, Deutschland und Spanien sowie in anderen europäischen Ländern, zum Beispiel: Italien, den Niederlanden, der Schweiz und Großbritannien.

Die Forschungsarbeit identifizierte zwei Haupttypen standortbezogener Systeme:

- die Vorhersage von „Hotspots“ für Straftaten, basierend auf historischen Polizeidaten, um zukünftige Tatorte vorherzusagen, und
- Algorithmen zur Vorhersage von Umgebungsrisiken, die auf der Annahme basieren, dass Umgebungsfaktoren den Ort von Straftaten bestimmen, und daher „riskante“ Orte vorhersagen können.

Methoden zur Vorhersage von „Hotspots“ für Straftaten nutzen historische Kriminalstatistiken darüber, wo und wann eine Straftat begangen wurde, um zukünftige Tatorte oder „Hotspots“ vorherzusagen. Diese Vorhersagen basieren auf der Analyse statistischer Erkenntnisse und Trends aus großen Mengen von Kriminalitätsdaten, häufig aus Polizeidatenbanken. Im Allgemeinen liefern Systeme zur Vorhersage von „Hotspots“ der Polizei eine „Heatmap“, um Gebiete oder Orte zu identifizieren, in bzw. an denen ein hohes Kriminalitätsrisiko besteht.

Systeme zur Vorhersage von „Hotspots“ für Straftaten dienen der Zuweisung von Polizeiressourcen und der Entscheidung, wo und wann Polizeikräfte patrouillieren sollen. Mögliche Ergebnisse in „Hotspot“-Gebieten sind Überwachung, Informationsbeschaffung, Identitätsprüfungen, Befragungen, Durchsuchungen, einstweilige Verfügungen, Hausdurchsuchungen und Festnahmen. Die Studie erhebt Bedenken, dass die als „Hotspots“ für Straftaten eingestuft Orte überproportional häufig Gebiete oder Viertel sind, in denen einkommensschwache und rassifizierte Bevölkerungsgruppen leben und arbeiten.

Standortbezogene Systeme basieren auf Umgebungs- und Kontextdaten. Sie nutzen Umgebungs- oder Kontextdaten, um Gebiete oder Orte zu identifizieren, die mutmaßlich anfälliger für Kriminalität



sind. Ein Algorithmus weist Orten einen Anfälligkeitswert zu, der auf räumlichen Faktoren basiert, darunter:

- ob der Ort gut beleuchtet ist,
- U-Bahn- oder Bushaltestellen,
- Café-Sitzbereiche im Freien,
- Fast-Food-Restaurants,
- öffentliche Toiletten,
- Apotheken, Bars, bestimmte Arten von Geschäften,
- Bäume und Bänke sowie
- Schulen und Postämter.

Diese Methode wirft ähnliche Probleme der Voreingenommenheit und Diskriminierung auf wie Systeme, die auf Kriminalitätsdaten basieren.

Personenbezogene Systeme zum Predictive Policing und zur Kriminalitätsvorhersage

Personenbezogene Instrumente zur Kriminalitätsvorhersage sollen die Wahrscheinlichkeit oder das Risiko, dass eine Person eine Straftat begeht, vorhersagen. Ähnliche Systeme werden eingesetzt, um die Wahrscheinlichkeit zu beurteilen, Opfer von Straftaten wie geschlechtsspezifischer Gewalt zu werden, oder um mutmaßlich falsche Anzeigen von Straftaten aufzudecken.

Die von diesen Systemen erfassten Personen werden einer ständigen Analyse von Daten unterzogen, die sie, ihr vergangenes und gegenwärtiges Leben sowie ihre Beziehungen charakterisieren. Ziel ist es, ihr Verhalten, ihr „Risiko“ oder ihre vermeintliche „Kriminalität“ zu bestimmen und „vorherzusagen“. Dies kann schwerwiegende Folgen haben. Die von diesen Systemen generierten Ergebnisse können zur Folge haben, dass Personen überwacht oder beobachtet werden. Sie können zu vermehrten Polizeikontrollen, Befragungen, Durchsuchungen, Haus- oder Arbeitsplatzbesuchen, Arbeitsverboten, Inhaftierungen, Abschiebungen oder Verhaftungen führen.

Diese Instrumente werden auch im Strafrechtssystem eingesetzt und können die Entscheidungsfindung von Richtern, einschließlich der



Urteilsverkündung, beeinflussen. Sie können die Dauer der Haftstrafe und den Zeitpunkt der Entlassung sowie die Haftbedingungen einer Person beeinflussen.

Fazit

Der Einsatz dieser Systeme führt zu rassistischer und sozioökonomischer Profilerstellung, Diskriminierung und Kriminalisierung. Dies richtet sich insbesondere gegen marginalisierte Personen und Gemeinschaften, insbesondere Schwarze und ethnische Minderheiten sowie Personen aus sozial schwachen Schichten.

Ihr Einsatz führt zu ungerechten und diskriminierenden Konsequenzen: von Überwachung, Identitätsprüfungen und Durchsuchungen über polizeiliche Schikanen und Hausdurchsuchungen bis hin zu Arbeitsverboten, Festnahmen, Inhaftierungen und Abschiebungen.

Diese Systeme werden im Verborgenen eingesetzt, d. h., die Menschen sind sich ihrer Nutzung nicht bewusst. Infolgedessen können betroffene Personen die Systeme und die Maßnahmen, die sich aus ihren Ergebnissen ergeben, nicht anfechten. Selbst wenn dies möglich wäre, gibt es keinen klaren Rahmen für die Rechenschaftspflicht.

Das Fazit aller Partnerberichte und dieses Berichts ist dasselbe: Diese Systeme müssen verboten werden.





Einleitung

In ganz Europa nutzen Polizei und Strafverfolgungsbehörden eine zunehmende Anzahl digitaler und datenbasierter Systeme. Neue Systeme werden mit schwindelerregender Geschwindigkeit eingeführt, ohne dass es eine transparente Darstellung ihres Einsatzes oder eine vorherige Berücksichtigung ihrer Auswirkungen und Folgen gibt.

Zu diesen Systemen gehören:

- Überwachung mit Gesichtserkennung,
- Systeme zur Emotionserkennung,
- Tools zur Extraktion von Daten von Mobiltelefonen,
- elektronische Markierungen und Fußfesseln sowie
- Vorhersage- und Profiling-Systeme.

All diesen Praktiken gemein ist die Erhebung und Verarbeitung riesiger Datenmengen – oft sensibler personenbezogener Daten – als Grundlage der Entscheidungsfindung.

Dieser Bericht konzentriert sich auf datenbasierte, algorithmische und automatisierte Systeme zur Entscheidungsfindung, die von der Polizei eingesetzt werden, um „vorherzusagen“, wo, wann und von wem Straftaten begangen werden. Befürworter

dieser vermeintlich wissenschaftlichen und „vorausschauenden“ Ansätze argumentieren, dass sie es der Polizei ermöglichen, die Effizienz ihrer Einsätze zu steigern und gleichzeitig Kosten zu senken:

„Durch die neue Strategie der evidenzbasierten Polizeiarbeit können Regierungen transparent mit Polizei und Öffentlichkeit zusammenarbeiten, um in kosteneffiziente Polizeiaufgaben zu investieren. Diese Investitionen können getätigt werden, während gleichzeitig die Polizeibudgets gekürzt werden, indem teure, aber ineffektive Polizeiaufgaben beendet werden.“⁷

Der KI-Koordinator der französischen *Gendarmerie Nationale*, Oberst Patrick Perrot, behauptet, datenbasierte Methoden ermöglichen es der Polizei, Verbrechen vorherzusehen, bevor sie geschehen:

„...der wissenschaftliche Ansatz ermöglicht es uns, Modellierungstechniken zu entwickeln, die zukünftige Entwicklungen verstehen und uns darauf vorbereiten können. Im Bereich der Kriminalität ist Antizipation heute ein entscheidender Faktor.“⁸

Dies hat wiederum zu einer verstärkten Überprüfung sogenannter Systeme zum Predictive Policing durch zivilgesellschaftliche Organisationen, politische Aktivisten und Organisatoren sowie Wissenschaftler in ganz Europa geführt.

Viele Gruppen äußern ernsthafte Bedenken hinsichtlich der möglichen Folgen dieser Systeme, beispielsweise Überwachung, Beobachtung, Befragung, Personenkontrollen, Geldstrafen, Hausdurchsuchungen, Gewaltanwendung, Abschiebung, Inhaftierung und Festnahme – sowie der möglichen Verletzungen individueller Rechte. Diese Systeme beeinträchtigen und verletzen möglicherweise das Recht auf ein faires Verfahren, Privatsphäre, Freiheit von Diskriminierung, die Unschuldsvermutung und das Recht auf einen wirksamen Rechtsbehelf.⁹

Die in diesem Bericht zusammengefassten Forschungsergebnisse verstärken diese Bedenken. Ziel ist es, Kampagnen auf internationaler, nationaler, regionaler und lokaler Ebene zu unterstützen, die ein Verbot des Einsatzes von KI und Algorithmen durch Strafverfolgungsbehörden fordern. Wo Verbote noch nicht eingeführt wurden, sind Verfahrensgarantien erforderlich, darunter strenge Tests vor der Einführung, Anforderungen an Transparenz gegenüber der Öffentlichkeit und wirksame Rechtsbehelfsmöglichkeiten.



Berichtsübersicht

In diesem Bericht werden umfassende Forschungsergebnisse zu Vorhersagesystemen und Datenbanken in Polizei- und Strafrechtssystemen in Europa zusammengefasst. Die Ergebnisse basieren auf Untersuchungen in vier Ländern: Belgien, Frankreich und Deutschland sowie Spanien.

Diese Länder wurden hauptsächlich aus zwei Gründen ausgewählt. Es war bekannt, dass Vorhersagesysteme bei Polizeikräften und im Strafrechtssystem weit verbreitet sind. Es gab jedoch nur wenige öffentlich zugängliche Forschungsergebnisse zur Entwicklung, Nutzung und Wirkung dieser Systeme.

Diese Studie wurde 2023 und 2024 von Forschenden von *AlgorithmWatch*, *La Quadrature du Net* und *Technopolice* durchgeführt. Die Originalversionen sind online verfügbar.¹⁰ Zusätzliche Untersuchungen zu Spanien wurden auch von *AlgoRace* durchgeführt.

In jedem Land arbeiteten Forschende daran, die eingesetzten Vorhersagesysteme, ihre Funktionsweise, ihre Ergebnisse und ihre Auswirkungen auf Personen, Gruppen und Gemeinschaften aufzudecken.

Diese Forschungsergebnisse werden in diesem Bericht zusammengefasst, um einen Überblick über die Landschaft, Trends und Folgen von Predictive Policing in Belgien, Frankreich, Deutschland und Spanien zu geben. Er umfasst zudem weitere Forschungsergebnisse und Berichte über den Einsatz von Systemen zur Vorhersage und zum Profiling in Polizei- und Strafrechtssystemen in anderen europäischen Ländern, darunter in den Niederlanden, Italien, der Schweiz und dem Vereinigten Königreich.

Der Bericht untersucht in vier Abschnitten die datenbasierten „Vorhersagesysteme“ der Polizei: standortbezogene Systeme, personenbezogene Systeme, KI-Videoüberwachung und Datenbanken. In jedem Abschnitt werden anhand einiger wichtiger Beispiele aus jedem Land die Zwecke, Dateneingaben und Ergebnisse der Systeme zusammengefasst.

Im letzten Abschnitt des Berichts werden die wichtigsten Bedenken und Verletzungen individueller Rechte, darunter Diskriminierung, Kriminalisierung, Transparenz, Rechenschaftspflicht und Rechtswidrigkeit analysiert.





Strukturelle und institutionelle Diskriminierung

Die meisten Systeme zur Kriminalitätsvorhersage nutzen historische Kriminalitätsdaten. Dies spiegelt den bestehenden institutionellen Rassismus, die Diskriminierung und die Vorurteile innerhalb der Polizei, der Strafverfolgungsbehörden und der Gesellschaft wider.

Die diskriminierenden Polizeipraktiken des rassistischen und ethnischen Profiling werden seit langem von Opfern, Opferverbänden, Wissenschaftlern, Menschenrechtsorganisationen und internationalen Organisationen kritisiert. Sie führen zu Kontrollen, Identitätsprüfungen und Durchsuchungen aufgrund rassifizierter Merkmale wie Hautfarbe oder (vermuteter) Religionszugehörigkeit.

Eine Studie der Agentur der Europäischen Union für Grundrechte aus dem Jahr 2017, im Rahmen derer Personen in jedem der damals 28 EU-Mitgliedstaaten befragt wurden, ergab, dass fast die Hälfte der Befragten aus bestimmten ethnischen Minderheiten von der Polizei angehalten wurde. Dazu gehörten Personen „mit subsaharischem afrikanischen Hintergrund“ in Luxemburg und Finnland, Personen mit „nordafrikanischem Hintergrund“ in den Niederlanden sowie Roma in Griechenland und Portugal.¹¹

Laut der Agentur der Europäischen Union für Grundrechte (FRA) empfand die Mehrheit

der in der EU von der Polizei angehaltenen Personen „afrikanischer Abstammung“ dies als rassistisch motiviert.¹² In Frankreich ist die Wahrscheinlichkeit, von der Polizei angehalten zu werden, für junge Männer, die als schwarz oder arabisch wahrgenommen werden, 20-mal (2000 %) so hoch wie für den Rest der Bevölkerung, so der Menschenrechtsbeauftragte des Landes.¹³

In Belgien gibt es einen Mangel an offiziellen Informationen zu ethnischen Profiling, da die Polizei bisher keine Verpflichtung hatte, die von ihr durchgeführten Kontrollen zu protokollieren. Amnesty International befragte jedoch belgische Polizeibeamte, die selbst zugaben, dass es in der Polizeiarbeit zu ethnischen Profiling kommt. Einer wurde folgendermaßen zitiert: „Ich nutze zwar ethnisches Profiling, aber ich weiß nicht, wie ich meine Arbeit anders machen soll. Wir müssen diskriminieren, sonst würden wir niemanden erwischen.“¹⁴

In Spanien werden überproportional viele Personen aufgrund ihrer rassischen, ethnischen oder religiösen Herkunft angehalten und durchsucht. Dies wurde durch mehrere Studien gut dokumentiert.¹⁵ Personen aus Nordafrika, Subsahara-Afrika und osteuropäischen Ländern werden häufiger Identitätskontrollen unterzogen als Spanier.¹⁶

In Deutschland sind Personen mit ausländischer Staatsangehörigkeit unter den von der Polizei erfassten Verdächtigen, den von Gerichten Verurteilten und den Inhaftierten überrepräsentiert.¹⁷ In Belgien ergab eine Studie, dass Personen vor Gericht, deren Name als muslimisch wahrgenommen wurde, häufiger verurteilt wurden als Personen mit einem als belgisch wahrgenommenen Namen, sofern alle anderen Bedingungen unverändert blieben.¹⁸ In Frankreich werden Ausländer dreimal so häufig in Untersuchungshaft genommen,¹⁹ während 45 % der in Belgien in Untersuchungshaft Inhaftierten keine belgischen Staatsbürger*innen sind.²⁰

Trotz dieser eindeutigen Beweise wird Diskriminierung durch die Polizei, Strafverfolgungsbehörden und das Strafrechtssystem in vielen europäischen Ländern noch immer nicht allgemein als strukturelles oder institutionelles Problem betrachtet oder anerkannt. Die schwarzen Autoren des Afrozensus 2020, einer Umfrage unter 6000 schwarzen, afrikanischen und afrodiasporischen Menschen in Deutschland, betonen:

„...die Öffentlichkeit beschäftigt sich nach wie vor mit der Frage, ob es innerhalb der deutschen Polizei tatsächlich institutionellen Rassismus gibt oder ob es sich vermeintlich um Einzelfälle handelt. Für schwarze, afrikanische und afrodiasporische Menschen stellt sich diese Frage nicht, für sie ist dies die Lebensrealität.“²¹

Diese Daten, die institutionelle und systemische Diskriminierung abbilden, werden von Strafverfolgungs- und Strafjustizbehörden in Systemen zur Vorhersage, zum Profiling und zur Risikobewertung verwendet.

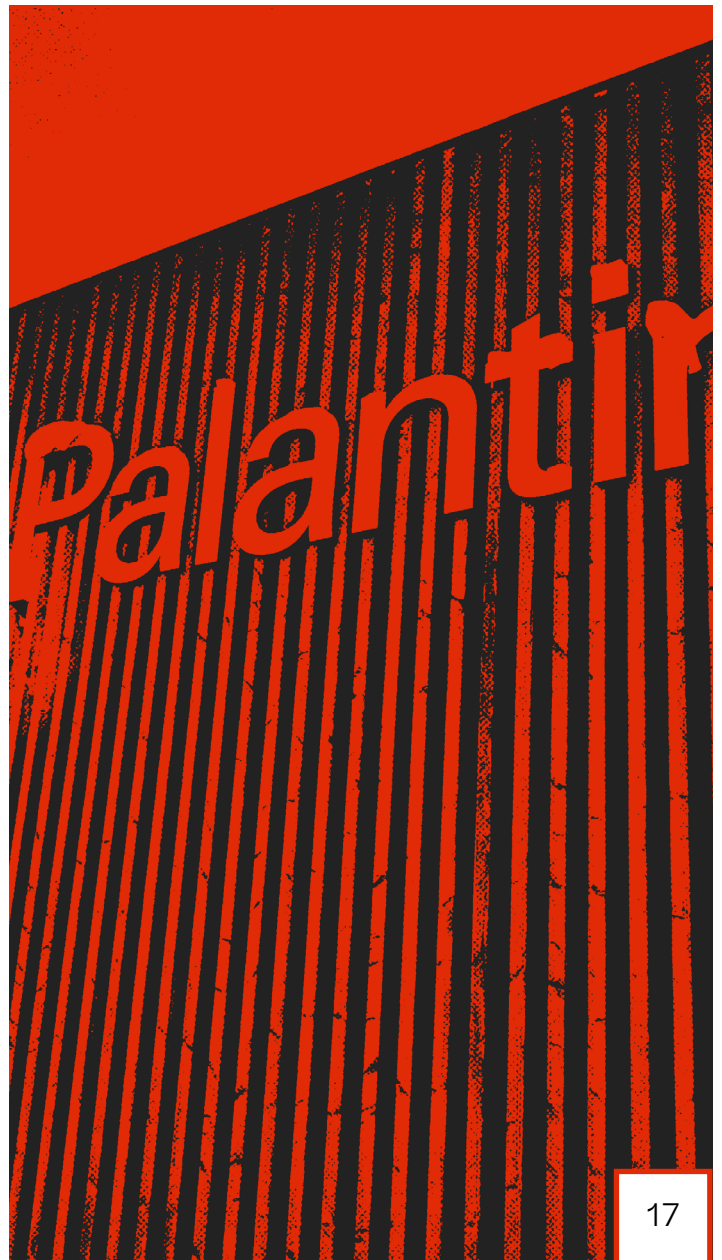
Unternehmensbeteiligung

Private Unternehmen spielen bei der Digitalisierung und Automatisierung der Polizeiarbeit eine wichtige Rolle. Viele der von Forschenden in Belgien, Frankreich und Deutschland identifizierten Systeme werden von privaten Sicherheitsunternehmen an Polizeikräfte geliefert, in der Regel im Rahmen wettbewerblicher Ausschreibungen. Andere datenbasierte Systeme werden intern oder in Zusammenarbeit mit wissenschaftlichen Forschenden entwickelt.

Der größte und berüchtigtste Technologiekonzern, der in Europa Software zum Predictive Policing verkauft, ist Palantir. Drei der 16 deutschen Bundesländer nutzen derzeit die Systeme des Unternehmens.²² Im Jahr 2024 belief sich der weltweite Umsatz von Palantir auf 2,87 Milliarden US-Dollar.²³ Das Unternehmen ist international für seine Verbindungen zu Geheimdiensten, dem Militär und anderen Regierungsbehörden bekannt.²⁴

Weitere wichtige Unternehmen, die datengesteuerte Systeme für Polizeikräfte in Europa bereitstellen, sind:

- Briefcam, ein israelisches Unternehmen, das KI-Videoüberwachungssysteme herstellt;²⁵
- ClearView, ein amerikanisches Unternehmen für Gesichtserkennung, das hauptsächlich Software für Strafverfolgungsbehörden anbietet;²⁶
- Edicia, ein französisches Unternehmen, das Software für „städtische Sicherheit“ entwickelt;²⁷
- Simsi, das mit der US-amerikanischen Rutgers University in New Jersey als kommerzieller Anbieter des Systems zum Risk Terrain Modelling zusammenarbeitet;²⁸
- EuroCop in Spanien, das in den letzten zwei Jahrzehnten über 100 Verträge mit öffentlichen Verwaltungsbehörden abgeschlossen hat;²⁹
- Securitas, ein schwedisches



Unternehmen, das „Sicherheitslösungen“ anbietet,³⁰ und

- SopraSteria, ein französisches Unternehmen, das auch Verträge mit der EU zur Entwicklung eines ihrer umfangreichen biometrischen Polizei- und Einwanderungssysteme hat.³¹

Neben Briefcam haben auch andere israelische Unternehmen Verträge mit belgischen Behörden, nämlich TA9/Rayzone und Interionet. Die Ursprünge von TA9 sind besonders besorgniserregend: Der CEO war zuvor stellvertretender Direktor der Einheit 8200, der Geheimdiensteinheit des israelischen Militärs, die angeblich für die Entwicklung der KI-Systeme der Armee verantwortlich ist.³² Mehrere Beamte, die später private Sicherheitsunternehmen gründeten, gehörten ursprünglich Einheit 8200 an.³³

Die Überwachungstechnologiebranche boomt derzeit.³⁴ Schätzungen zufolge beträgt die jährliche weltweite Wachstumsrate 12,5 %, was einem Branchenwert von 186 Milliarden US-Dollar im Jahr 2025 entspricht.³⁵ Angesichts der offensichtlichen Lukrativität dieser Branche ist davon auszugehen, dass die Anzahl der Vorhersagesysteme und der Unternehmen, die sie anbieten, in den kommenden Jahren zunehmen wird.

1.4. Die Verordnung der Europäischen Union zur künstlichen Intelligenz (KI-Verordnung der EU)

Die KI-Verordnung der EU ist ein globaler Meilenstein in der Regelung von KI, basierend auf den potenziellen Risiken für Gesundheit, Sicherheit und Grundrechte. Sie wurde im Juni 2024 nach langwierigen und komplexen Verhandlungen im Europäischen Parlament



verabschiedet. Die ersten Teile der Verordnung traten im Februar 2025 in Kraft.

Die KI-Verordnung legt eine Reihe „verbotener KI-Praktiken“ fest. Dazu gehören:

- „Predictive Policing“,
- biometrische Fernidentifizierung (z. B. Gesichtserkennung),
- „Social Scoring“ und
- Emotionserkennung.³⁶

Das Verbot von Systemen zur Kriminalitätsvorhersage ist vage und unklar und enthält eine umfassende Ausnahmeregelung, die seine Wirkung erheblich einschränken wird. Es ist möglich, dass viele, wenn nicht alle der in diesem Bericht behandelten Systeme und die zugrunde liegenden Forschung³⁷ nicht durch die Verordnung verboten werden. In Bezug auf Systeme zum Predictive Policing verbietet die Verordnung:

„...das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung eines KI-Systems zur Durchführung von Risikobewertungen in Bezug auf natürliche Personen, um das Risiko, dass eine natürliche Person eine Straftat begeht, ausschließlich auf der Grundlage des Profiling einer natürlichen Person oder der Bewertung ihrer persönlichen Merkmale und Eigenschaften zu bewerten oder vorherzusagen.“

Doch weiter heißt es:

„...dieses Verbot gilt nicht für KI-Systeme, die dazu verwendet werden, die durch Menschen durchgeführte Bewertung der Beteiligung einer Person an einer kriminellen Aktivität, die sich bereits auf objektive und überprüfbare Tatsachen stützt, die in unmittelbarem Zusammenhang mit einer kriminellen Aktivität stehen, zu unterstützen.“³⁸

Die Verordnung scheint *manche* KI-Systeme zu verbieten, die Vorhersagen über Personen auf der Grundlage der „Profilerstellung ... von Persönlichkeitsmerkmalen oder -eigenschaften“ treffen. Es gilt jedoch nicht für KI-Systeme, die menschliche Beurteilungen „unterstützen“. Diese späte Ergänzung des Textes macht das Verbot praktisch bedeutungslos. Die Strafverfolgungsbehörden können, wie bereits geschehen, einfach erklären, dass ihr Einsatz von KI-Systemen der „Unterstützung“ menschlicher Beurteilungen dient.

Darüber hinaus enthält der Text keine eindeutige Bezugnahme auf ortsbezogene oder geografische Systeme zur Kriminalitätsvorhersage, die in ganz Europa weit verbreitet sind, und verbietet diese auch nicht. Die Leitlinien der Europäischen Kommission zu verbotenen KI-Praktiken stellen klar, dass diese nicht unter das Verbot fallen³⁹ Die Leitlinien sind

jedoch nicht bindend. Sollten derartige Systeme rechtlich angefochten werden, könnte der Gerichtshof der Europäischen Union (EuGH) das letzte Wort haben.

Das Verbot wurde als lediglich „teilweises“ Verbot beschrieben und ist deutlich schwächer als die ursprüngliche Fassung, die das Europäische Parlament im Juni 2023 verabschiedete.⁴⁰ Die Regierungen der EU-Länder und die großen Technologieunternehmen haben hart daran gearbeitet, die Schutzmaßnahmen in der Verordnung abzuschwächen.⁴¹

Die KI-Verordnung enthält einige sehr grundlegende Transparenzmaßnahmen. Sie sieht vor, dass in bestimmten Fällen, in denen Systeme als „hochriskant“ eingestuft werden, die Menschen über den Einsatz eines KI-Systems informiert werden sollen.⁴² Wenn eine Person einer Entscheidung unterworfen wird, die auf den Ergebnissen eines Hochrisiko-KI-Systems beruht, die Rechtswirkung hat oder die Person in einer Weise beeinträchtigt, die ihrer Ansicht nach nachteilige Auswirkungen auf ihre Gesundheit, Sicherheit oder Grundrechte hat, hat sie das Recht auf eine „klare und aussagekräftige Erklärung“ der Rolle des KI-Systems bei dieser Entscheidung.⁴³

Es gibt jedoch eine wichtige Ausnahme für Systeme, die zur Aufdeckung, Verhütung, Untersuchung und Verfolgung von Straftaten eingesetzt werden.⁴⁴ Infolgedessen enthält die Verordnung praktisch keine Transparenzmaßnahmen für Systeme zum Predictive Policing und Systeme zur Kriminalitätsvorhersage.

Darüber hinaus gibt es keinen sinnvollen Mechanismus, mit dem Betroffene einer „verbotenen KI-Praxis“ oder von KI-Systemen, die nicht der Verordnung entsprechen, diese Systeme anfechten oder Wiedergutmachung für die durch den Einsatz von KI-Systemen entstehenden Schäden verlangen können.⁴⁵ Betroffene können sich bei einer nationalen Behörde beschweren, die Verordnung verpflichtet diese Behörden jedoch nicht, Abhilfe zu schaffen.⁴⁶

In der bestehenden Datenschutzgesetzgebung gibt es Standards, nämlich in der Datenschutz-Grundverordnung (DSGVO) und der Richtlinie (EU) 2016/680. Letztere gilt für die Nutzung von Daten und automatisierte Entscheidungsfindungssysteme durch Strafverfolgungsbehörden. Die Richtlinie (EU) 2016/680 verbietet Entscheidungen, die *ausschließlich* auf automatisierter Verarbeitung beruhen. Wie bereits erwähnt, kann dies das Verbot jedoch bedeutungslos machen. Strafverfolgungsbehörden können einfach behaupten, die Entscheidungen beruhten nicht ausschließlich auf automatisierter Verarbeitung.



1.5. Methodik

Die diesem Bericht zugrunde liegende Forschungsarbeit zu Belgien, Frankreich, Deutschland und Spanien wurde von Forschenden und Ermittler*innen in diesen Ländern unter Einsatz einer Reihe von Methoden durchgeführt. Unterstützt wurden sie von den Herausgeber*innen dieses Berichts.

- **Interviews:** Die Forschenden führten Interviews mit Expert*innen, Wissenschaftler*innen und anderen Forschenden sowie mit Entwickler*innen der datenbasierten und automatisierten Entscheidungssysteme. Sie befragten darüber hinaus Polizeibeamte und andere für den Betrieb dieser Systeme verantwortliche Beamte. Besonders wichtig war die Befragung von Personen und Gruppen, die von diesen Systemen und dem von ihnen beeinflussten polizeilichen und strafrechtlichen Handeln betroffen sind, sowie von Personen, die mit diesen Gruppen zusammenarbeiten.
- **Anfragen im Rahmen der Gesetzgebung zur Informationsfreiheit:** Die Forschenden nutzten die Gesetze zur Informationsfreiheit, um Anfragen an lokale und nationale Polizeikräfte, Behörden sowie Strafvollzugs- und Bewährungsbehörden zu richten.
- **Open-Source-Recherche:** Die Forschenden durchsuchten öffentliche Dokumente wie Verträge, Finanzunterlagen, interne Evaluierungsberichte und Studien, Folgenabschätzungen, Unternehmenswebsites und -broschüren sowie verwandte Informationen.
- **Durchsicht vorhandener wissenschaftlicher Literatur:** Die Forschenden überprüften und analysierten Studien und Berichte zu diesen Systemen, insbesondere technische Studien zu deren Design, Schulung und Betrieb.

Transparenzprobleme

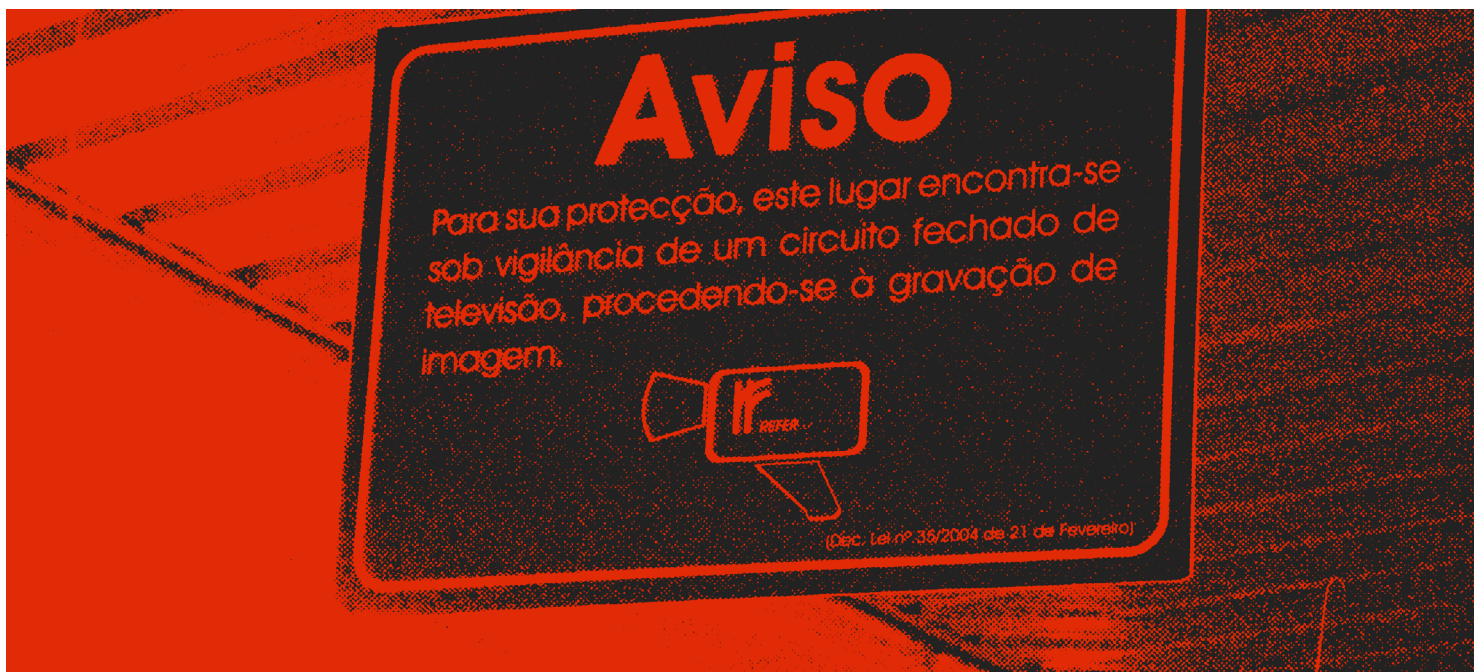
Aus allen Länderstudien geht hervor, dass Polizei und Strafverfolgungsbehörden die Veröffentlichung von Informationen über Systeme zur Vorhersage, zum Profiling und zur Risikobewertung einschränken und verhindern wollen.

In allen Ländern wurden formelle Anfragen von Forschenden an Behörden, Polizeikräfte und lokale Behörden abgelehnt oder ignoriert – oft mit der Begründung, sie seien mit Geschäftsgeheimnissen oder einer Bedrohung der nationalen Sicherheit verbunden.⁴⁷ Wenn Behörden reagierten, waren die Informationen oft spärlich und ausweichend.⁴⁸ Private Unternehmen stellen der Polizei wichtige Infrastruktur und operative Instrumente zur Verfügung. Sie fallen jedoch nicht unter die Gesetze zur Informationsfreiheit.⁴⁹

Ebenso wurden Interviewanfragen oft abgelehnt oder ignoriert. In Spanien stellte *AlgoRace* mehrere Interviewanfragen an Regierungsbehörden. Diese wurden abgelehnt, obwohl die Personen, an die die Anfragen gerichtet waren, sich bereit erklärten, einzeln zu sprechen.

Das Maß an Transparenz in Bezug auf diese Systeme ist völlig inakzeptabel, insbesondere angesichts der schwerwiegenden technischen, rechtlichen und politischen Probleme, die sie aufwerfen.





Systeme zur standortbezogenen Vorhersage

Methoden des standortbezogenen Predictive Policing werden entwickelt, um vorherzusagen, wo und oft auch wann ein Verbrechen geschehen wird, um Polizeiressourcen an diesen Orten einzusetzen. Die Forschungspartner*innen fanden in allen Fokusländern Beispiele für Algorithmen zur geografischen Kriminalitätsvorhersage: Belgien, Frankreich, Deutschland und Spanien.

Befürworter*innen standortbezogener Systeme zum Predictive Policing behaupten, datenbasierte Ansätze könnten die Polizeiarbeit effizienter gestalten. Durch die Identifizierung der Orte mit den größten Gefahren, so das Argument, könne die Polizei Verbrechen verhindern. Dieser Ansatz wurde wie folgt zusammengefasst:

„Wenn die Polizei ihre Ressourcen gezielt auf diese risikobehafteten Personen, Orte und Zeiten konzentrieren kann, kann sie die Kriminalität in ihrem Zuständigkeitsbereich effektiver reduzieren.“⁵⁰

In Europa haben Forschende zwei Haupttypen standortbezogener Systeme identifiziert:

- Algorithmen zur Vorhersage von „Hotspots“ für Straftaten, basierend auf historischen Polizeidaten, um zukünftige Tatorte vorherzusagen, und

- Algorithmen zur Vorhersage von Risiken, die auf der Annahme basieren, dass Umgebungsfaktoren den Ort von Straftaten bestimmen.

Beide Methoden geben Anlass zur Sorge hinsichtlich der unverhältnismäßigen gezielten Verfolgung und Kriminalisierung von Personen und Gemeinschaften aus ethnischen Minderheiten und mit niedrigem Einkommen.

Die in diesem Bericht skizzierten Beispiele zeigen, dass standortbezogenes Predictive Policing schwerwiegende Folgen für Personen haben kann, die in Gebieten leben und arbeiten, die als risikoreich eingestuft wurden. Sie können verstärkt polizeilicher Überwachung, Beobachtung, Fahrzeug- und Identitätskontrollen, Durchsuchungen, Befragungen und sogar Verhaftungen ausgesetzt sein.

Obwohl die KI-Verordnung der EU ein formales Verbot bestimmter Arten von Systemen zum Predictive Policing vorsieht, erstreckt es sich gemäß den offiziellen Richtlinien nicht auf Systeme zur standortbezogenen Vorhersage.⁵¹ Die Forschungsergebnisse verdeutlichen das Diskriminierungs- und Profiling-Potenzial dieser Systeme. Sie müssen in jedes sinnvolle Verbot von Predictive Policing einbezogen werden.

Dieser Bericht ist lediglich eine Momentaufnahme der von Polizeikräften in ganz Europa eingesetzten geografischen Systeme zur Kriminalitätsvorhersage. Neben den Systemen in Frankreich, Belgien, Deutschland und Spanien gibt es – wie frühere Untersuchungen gezeigt haben – auch ähnliche Beispiele in Italien, der Schweiz und dem Vereinigten Königreich.

Vorhersage von „Hotspots“ für Straftaten

Ortsbezogene Systeme in Belgien, Frankreich, Deutschland und Spanien nutzen überwiegend Methoden zur Vorhersage von „Hotspots“ für Straftaten. Hierbei werden historische Kriminalstatistiken, die zeigen, wo und wann Straftaten begangen wurden, genutzt, um zukünftige Tatorte oder „Hotspots“ vorherzusagen.

Die Forschenden identifizierten mindestens neun verschiedene Systeme zur Vorhersage von „Hotspots“. Viele davon werden von mehreren Polizeibehörden in den einzelnen Ländern eingesetzt.

In Deutschland:

- Die Berliner Polizei verfolgt eine Strategie zur Klassifizierung *kriminitätsbelasteter Orte* (kbOs), an denen erweiterte Polizeibefugnisse genutzt werden können;⁵²
- drei deutsche Bundesländer nutzen aktuell „Hotspot“-Systeme für Straftaten, während im Jahr 2018 sechs Bundesländer fünf verschiedene Systeme nutzten.⁵³
- Diese Systeme sind:

- SKALA (System zur Kriminalitätsauswertung und Lageantizipation) in Nordrhein-Westfalen;
- KrimPro (Kriminalitätsprognose Wohnraumeinbruch) in Berlin und
- KLB-operativ (*Kriminalitätslagebild*) in Hessen⁵⁴ und
- Die bayerische Polizei nutzt das Pre-Crime Observation System (PRECOBS).⁵⁵

Systeme zur standortbezogenen Vorhersage sind in Spanien weit verbreitet:

- Das „Predictive Police Patrolling Decision Support System“ (P3-DSS) wird landesweit eingesetzt⁵⁶ und
- sieben verschiedene Regionen nutzen ein EuroCop-System, darunter fast alle Polizeikräfte in Madrid.⁵⁷

In Frankreich und Belgien fanden die Forschenden weniger aktive Beispiele für Hotspot-Polizeimethoden. In Frankreich identifizierte *La Quadrature du Net* „PredVol“ und PAVED, die beide von der *Gendarmerie Nationale* eingesetzt, aber inzwischen eingestellt wurden.⁵⁸

In Belgien identifizierte *TechnoPolice* einen kleinen Versuch der Westkust-Polizei und den Einsatz des geografischen Informationssystems der Firma Orbit in Flandern und Brüssel.⁵⁹ Orbit behauptet, seine Software sei „bereits in fast 100 Polizeizonen im Einsatz“.⁶⁰

Vorhersagesysteme für „Hotspots“ für Straftaten sind international auf breite Kritik gestoßen, nachdem das PredPol-System in den USA wegen der Verstärkung und Aufrechterhaltung rassistischer Vorurteile geprüft wurde.⁶¹

Die in diesem Bericht behandelten Systeme, von denen einige weitgehend ähnliche Methoden wie PredPol verwenden, geben in Bezug auf Diskriminierung und Kriminalisierung ebenfalls Anlass zur Sorge. In allen vier Ländern sind die von den „Hotspot“-Systemen für Straftaten als „Hochrisikogebiete“ eingestuften Gebiete häufig Gebiete, in denen marginalisierte Bevölkerungsgruppen leben und arbeiten.

Zwecke

Die Polizei behauptet, dass sie mithilfe statistischer Berechnungen zur Vorhersage von „Hotspots“ für Straftaten die Kriminalitätsrate senken kann. Florian Gauthier, der französische Datenwissenschaftler und Entwickler von PredVol, begründet die Notwendigkeit von „Hotspot“-Polizeiarbeit zur Vorhersage von Autodiebstählen mit den Diskrepanzen zwischen den Orten, an denen Polizeikräfte patrouillieren, und den Orten, an denen Autodiebstähle stattfinden. Diese Diskrepanzen, so Gauthier, könnten durch die Nutzung von Kriminalitätsdaten zur Steuerung der Streifen reduziert werden.⁶²

Angeblich ermöglichen „evidenzbasierte“ Methoden den Einsatz von Polizeikräften zur richtigen Zeit am richtigen Ort und verhindern so kriminelle Aktivitäten, bevor sie überhaupt stattfinden. In Deutschland behauptet die Berliner Polizei, dass die Ausweisung eines Gebiets als kbO das „Sicherheitsgefühl“ erhöht, da die Polizei dadurch „die Identität relevanter Personen kontrollieren, das Entdeckungsrisiko erhöhen und so Straftaten verhindern“ kann.⁶³

Viele der identifizierten „Hotspot“-Systeme, die von der Polizei eingesetzt werden, sind auf mutmaßliche Diebstähle oder Einbrüche ausgerichtet:

- In Frankreich ist PredVol auf mutmaßliche Autodiebstähle und PAVED⁶⁴ auf Autodiebstahl und Einbruch spezialisiert;
- in Deutschland konzentriert sich das System PRECOBS auf mutmaßlichen Fahrzeugdiebstahl und Einbruch, während sich mit dem KbO-System unter anderem auf Raubdelikte konzentriert wird;⁶⁵ Forschende vermuten, dass „Hotspot“-Systeme für Einbrüche in den 2010er-Jahren als Reaktion auf die Medienpanik über Einbrüche eingeführt wurden;⁶⁶
- in Belgien konzentriert sich das Vorhersagesystem der örtlichen Westkust-Polizei auf Einbruch und Fahrzeugdiebstahl⁶⁷ und
- in Spanien wird versucht, mit dem EuroCop-System Diebstähle und andere Straftaten vorherzusagen;⁶⁸

Genutzte Daten

Systeme zur Vorhersage von „Hotspots“ für Straftaten gewinnen statistische Erkenntnisse und Trends aus großen Mengen an Kriminalitätsdaten, häufig aus Polizeidatenbanken, um zukünftige Tatorte vorherzusagen.

In Deutschland setzt das Modell zur standortbezogenen Kriminalitätsvorhersage kbO (*Kriminalitätsbelastete Orte*) eine statistische Auswertung ein, die Kriminalitätsdaten und weitere, nicht näher spezifizierte Zusatzinformationen umfasst.⁶⁹

In Belgien nutzt das geografische Informationssystem Orbit, das offenbar von mehr als 100 lokalen Polizeidienststellen genutzt wird, frühere Polizeiberichte zu Straftaten, um zukünftige „Hotspots“ zu identifizieren.⁷⁰ Das System der lokalen Polizei Westkust-Polizei nutzt ebenfalls Polizeidaten zu mutmaßlichen Straftaten, Kennzeichen, Gerichtsakten und sogar das Wetter.⁷¹

In Frankreich greift das System PredVol auf Daten über Autodiebstähle aus den IT-Systemen zurück, die zur Erfassung aller Anzeigen und Berichte verwendet werden, darunter:

- XY-Koordinaten des Orts des Autodiebstahls,
- Datum und

— zusätzliche Informationen zu Fahrzeugmodell und -farbe.⁷²

In Spanien kann das EuroCop-System auf verschiedene Informationsquellen zurückgreifen und diese integrieren, darunter polizeiliche Kriminalitätsdaten und -akten, sozioökonomische Daten sowie Videoüberwachungsdaten. Diese Daten werden in einem algorithmischen Modell kombiniert, um Kriminalität vorherzusagen und „Heatmaps“ und „Patrouillenrouten“ für die Polizei zu erstellen.⁷³

Es bestehen ernsthafte Bedenken, dass historische Polizeidaten in „Hotspot“-Systemen für Straftaten zu unrechtmäßiger Diskriminierung führen könnten. Wie im Folgenden erläutert wird, spiegeln historische Kriminalitätsdaten die übermäßige Polizeipräsenz und Kriminalisierung rassifizierter und einkommensschwacher Bevölkerungsgruppen wider. Algorithmen für „Hotspots“ für Straftaten bringen diese Unverhältnismäßigkeit und Diskriminierung in zukünftige Vorhersagen ein.

In der Tat räumte der belgische Innenminister im Juni 2020 ein: „Polizeistatistiken spiegeln in erster Linie die Polizeitätigkeit wider. Sie spiegeln nicht die tatsächliche Kriminalität in einem bestimmten Gebiet wider.“⁷⁴

Viele „Hotspot“-Systeme nutzen in ihren Trainingsdatensätzen auch soziodemografische Daten. Der Entwickler von PredVol erklärte gegenüber *La Quadrature du Net*, dass das System 600 soziodemografische Variablen verwendet. Dazu gehören Schulbesuchs- und Arbeitslosenquoten, die Anzahl der Geschäfte in der Nähe und das Durchschnittsalter der Bevölkerung. Die Behörden wollten keine umfassenderen Informationen bereitstellen.⁷⁵ Sie stellten außerdem fest, dass PAVED neben 15 soziodemografischen Variablen auch Daten zu Geschlecht, Staatsangehörigkeit und Einwanderungsstatus, Haushaltseinkommen und Bildungsniveau berücksichtigte.⁷⁶



Das „Smart Patrolling“-System P3DSS der spanischen Nationalpolizei nutzte ebenfalls Daten zur Staatsangehörigkeit und teilte die Einwohner Madrids in Gruppen ein: spanische Staatsbürger*innen, andere EU-Bürger*innen, Nicht-EU-Bürger*innen und – ungewöhnlicherweise – Bürger*innen nach Kontinenten.⁷⁷ Das System berechnete dann für jede Nationalitätengruppe ein „Polizeikontaktziel“: die jeder Gruppe zugeteilte Patrouillenzeit, basierend auf ihrer Größe im Verhältnis zum geografischen Gebiet.⁷⁸ Diese demografischen Gruppen sind zwar stark verallgemeinert, stellen aber im Wesentlichen Platzhalter für ethnische Gruppen dar.

Daten zu Staatsangehörigkeit, Einwanderungsstatus und Geschlecht sind allesamt „besondere Kategorien“ personenbezogener Daten oder können als solche betrachtet werden.⁷⁹ Diese und andere soziodemografische Variablen bergen das Risiko, Korrelationen zwischen Kriminalität und ethnischer Zugehörigkeit oder wirtschaftlicher Benachteiligung herzustellen. Das EU-Datenschutzrecht stellt klar:

„Ein Profiling, das zur Folge hat, dass natürliche Personen aufgrund von personenbezogenen Daten diskriminiert werden, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, sollte [...] verboten werden.“⁸⁰

Auf Grundlage dieser Eingabedaten verwenden „Hotspot“-Systeme statistische Analysen, um die Wahrscheinlichkeit zukünftiger Tatorte vorherzusagen. Die spezifischen Modellierungstechniken für diese geografischen und zeitlichen Analysen unterscheiden sich je nach System.

PAVED und PredVol nutzen maschinelles Lernen, d. h., die Systeme „lernen“ automatisch aus zusätzlichen Daten, ohne manuell neu trainiert werden zu müssen. Die meisten anderen „Hotspot“-Systeme in Belgien, Frankreich, Deutschland und Spanien nutzen algorithmische Methoden.

Ergebnisse

Im Allgemeinen liefern Systeme zur Vorhersage von „Hotspots“ der Polizei eine „Heatmap“, um Gebiete oder Orte vorherzusagen, in bzw. an denen ein hohes Kriminalitätsrisiko besteht. In Deutschland zeigt PRECOBS beispielsweise eine Karte mit unterschiedlich gefärbten Gebieten an. Diese stellen die angenommene Wahrscheinlichkeit bzw. das Risikoniveau dar, dass in diesem Gebiet eine Straftat begangen wird (siehe Abbildung 1).

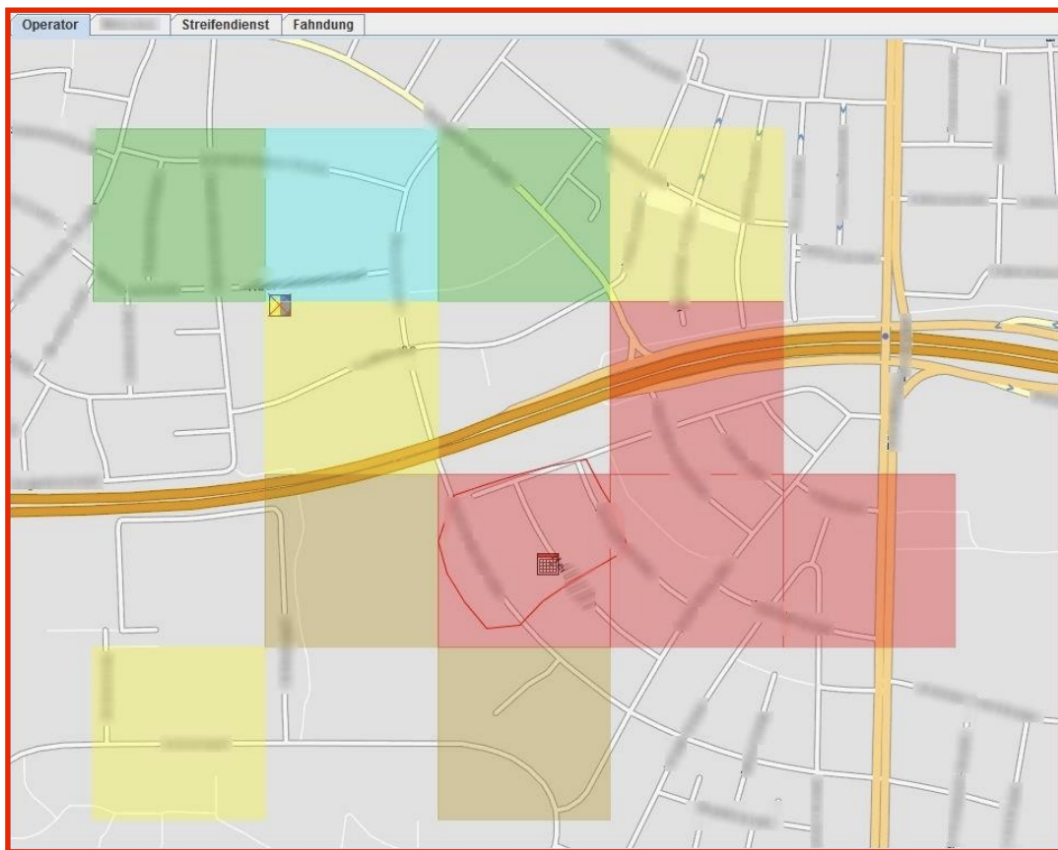


ABBILDUNG 1: SCREENSHOT DER VON PRECOBS ERSTELLTEN FARBKODIERTEN KARTE EINES STANDORTS. QUELLE: SONJA PETERANDERL

Manche Systeme, wie beispielsweise PredVol in Frankreich, sind für Beamte „auf der Straße“ auf Tablets zugänglich. Andere Systeme, wie beispielsweise PAVED, sind nur für Kommandeure zugänglich. Neben „Heatmaps“ bietet PAVED den Beamten auch Histogramme mit den soziodemografischen Variablen, die als einflussreichste Indikatoren für Kriminalität gelten (siehe Abbildung 2).

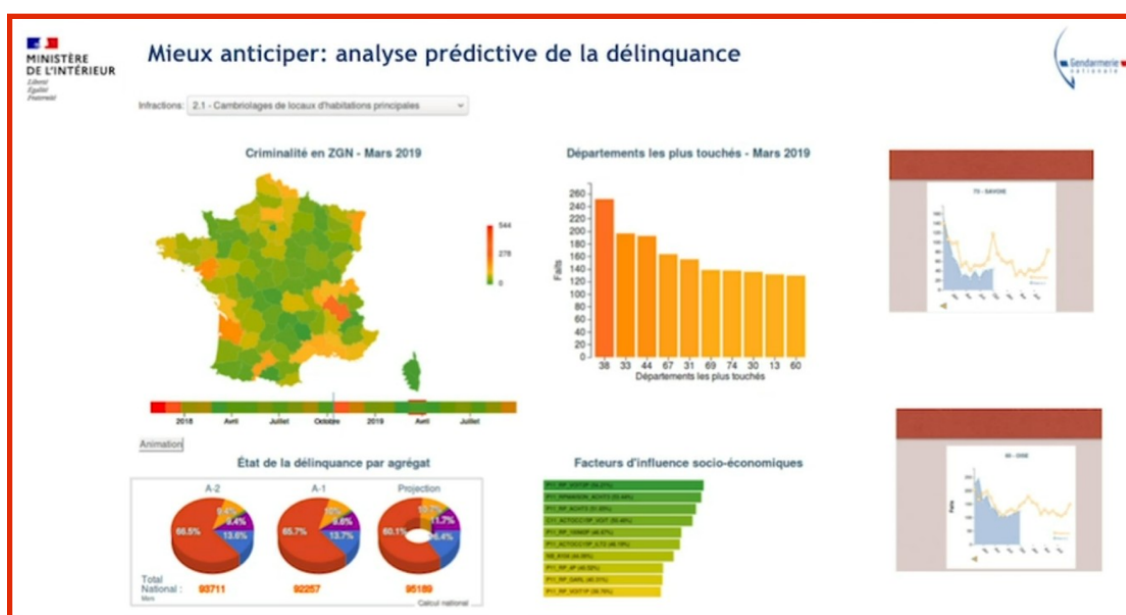


ABBILDUNG 2: SCREENSHOT DES VORTRAGS VON OBERST PATRICK PERROT, COLLOQUE DE L'INSTITUT DE DROIT PRIVÉ – UT CAPITOLE – 8. SEPTEMBER 2021 (QUELLE: „AI ET ENJEUX DE SÉCURITÉ“, MINUTE 23:10).

Systeme zur Vorhersage von „Hotspots“ für Straftaten dienen der Zuweisung von Polizeiressourcen und der Entscheidung, wo und wann Polizeikräfte patrouillieren sollen. Ergebnisse in Hotspot-Gebieten können sein:

- Überwachung,
- Informationsbeschaffung,
- Identitätsprüfungen,
- Befragungen,
- Durchsuchungen,
- einstweilige Verfügungen oder
- Festnahmen.⁸¹

Die Ausweisung von „Hotspot“-Gebieten kann auch erweiterte polizeiliche Befugnisse an diesen Orten ermöglichen. In Berlin ist es der Polizei gesetzlich gestattet, in sogenannten „kbOs“ Identitätsprüfungen oder Durchsuchungen von Personen oder Gegenständen ohne konkreten Verdacht, sondern „verhaltensabhängig“ durchzuführen.⁸²

La Quadrature du Net sprach mit einer Quelle, die erklärte, dass die von PAVED generierten „Hotspots“ genutzt würden, um Staatsanwälte zu bewegen, an diesen Orten spezielle Befehle für Identitäts- und Fahrzeugkontrollen zu erlassen. Diese ermöglichten es der Verwaltungspolizei, richterliche Befugnisse im Kontext polizeilicher Maßnahmen auszuüben – ein schwerwiegender Verstoß gegen die Pflichten der Verwaltungspolizei.⁸³



Auswirkungen

Orte, die von algorithmischen Systemen als „Hotspots“ für Straftaten eingestuft werden, sind überproportional häufig Gebiete oder Viertel, in denen einkommensschwache und rassifizierte Gruppen leben und arbeiten. Die Rechtsexpertin Lina Schmid weist darauf hin, dass als „kbOs“ eingestufte Orte in der Regel von einem hohen Anteil an Personen frequentiert werden, die als Migrant*innen wahrgenommen werden.⁸⁴

Nach der Einführung des PRECOBS-Systems in Bayern sagte Matthias Monroy, Herausgeber der deutschen Fachzeitschrift *Bürgerrechte & Polizei*:

„Wen kontrolliert die Polizei häufiger, wenn sie davon ausgeht, dass in den nächsten Stunden oder Tagen ein Einbruch bevorsteht? Ich würde sagen, es sind eher Menschen in schmutziger Kleidung, Menschen anderer Hautfarbe oder mit Kapuzenpullis – Muster, die es bei der Polizei bereits gibt.“⁸⁵

In Deutschland sind Kontrollen der Polizei aufgrund der einer Person zugeschriebenen Rasse verfassungsrechtlich verboten (Artikel 3 des Grundgesetzes). Lina Schmid erklärt jedoch, dass die Ausweisung bestimmter Gebiete als „Hotspots“ für Straftaten es der Polizei ermögliche, dieses Verbot zu umgehen:

„Kriminalisiert werden hier – statt rassifizierter Personengruppen, wie es bei Racial Profiling üblich ist – ganze Orte und die Personen, die sich dort aufhalten. Das eröffnet der Polizei Raum für verdecktes Racial Profiling, denn: Selbst wenn vermeintlich alle Menschen kontrolliert werden, ... sind es in der Praxis aber immer noch vor allem BIPOC [Schwarze, Indigene und People of Colour], die im Visier der Polizei stehen.“⁸⁶

Die Anwohnerinitiative *Wrangelkiez United* erklärte, dass die Kontrollen im Görlitzer Park/ Wrangelkiez kbO fast ausschließlich schwarze und rassistisch marginalisierte Personen betreffen, „unabhängig davon, was sie tun oder wohin sie gehen.“⁸⁷ Schüler einer Sprachschule im Viertel werden auf dem Weg zum Unterricht kontrolliert, und schwarze Männer erleben regelmäßig Kontrollen im Park, wie in Videointerviews mit *Wrangelkiez United* berichtet wird:

„Wenn die Polizei da ist (...), dann werden dunkelhäutige Menschen wie ich ohne wirklichen Grund kontrolliert – es liegt nicht daran, dass wir Straftaten begangen hätten. Es liegt an unserem Aussehen.“⁸⁸

Risikovorhersage

Standortbezogene Systeme in Europa umfassen auch Risikovorhersagesysteme, die auf Umgebungs- oder Kontextdaten zurückgreifen, um Orte mit einem vermeintlich höheren Kriminalitätsrisiko zu identifizieren.

Diese Systeme zur Vorhersage von umgebungsbezogenem Risiko basieren auf der kriminologischen „Broken Windows“-Theorie. Diese Theorie geht davon aus, dass die physische Umgebung ein entscheidender Faktor für Kriminalität ist. Sie wurde 1982 in den USA von James Wilson und George Kelling eingeführt.⁸⁹ Die Theorie basiert auf Annahmen über Umgebungsfaktoren (wie zerbrochene Fenster) als Indikatoren oder Abschreckungsmittel für Kriminalität.

Die „Broken Windows“-Theorie wurde später von der gesamten US-Polizei übernommen. Ein oft zitiertes Beispiel sind die vom ehemaligen New Yorker Polizeichef William Bratton eingeführten Änderungen.⁹⁰ Die Theorie hat seitdem die Gestaltung und Entwicklung datenbasierter Polizeimethoden beeinflusst, obwohl sie von Kriminologen und Soziologen weitgehend diskreditiert wurde.⁹¹

Ähnlich wie Algorithmen zur Erkennung von „Hotspots“ für Straftaten können auch Algorithmen zur Bestimmung von Umgebungsrisiken die Polizei in wirtschaftlich schwächere Stadtgebiete lenken, in denen sich eher rassifizierte Gruppen aufhalten bzw. in denen solchen Gruppen leben.

Zwecke

Die belgische und die französische Polizei nutzen ein algorithmisches Modell namens „Risk Terrain Modelling“ zur Vorhersage von Kriminalität, das auch die Bewertung von Umgebungsrisiken einschließt. Es gibt weitere bekannte Einsatzmöglichkeiten bei der britischen Polizei.⁹²

Die Risk-Terrain-Modelling-Methode (RTM-Methode) wurde von Joel Caplan und Leslie Kennedy, zwei Wissenschaftlern der Rutgers University in New Jersey, USA, entwickelt. Sie wurde Berichten zufolge in über 45 Ländern auf sechs Kontinenten getestet. Auf der Website von Risk Terrain Modelling, die für die Software der Firma Simsi wirbt, heißt es:

„Risk Terrain Modeling (RTM) identifiziert die Risiken, die von Landschaftsmerkmalen ausgehen, und modelliert, wie diese zusammenwirken und so einzigartige Verhaltensmuster für Kriminalität schaffen.

Sie können sich wahrscheinlich die klischeehafte „dunkle Gasse“ vorstellen, wenn Sie an potenzielle Orte für kriminelle Aktivitäten denken. In diesem Fall

werden mindestens zwei Landschaftsmerkmale berücksichtigt: (1) eine Gasse und (2) schlechte Beleuchtung. An Orten, an denen diese besonderen Merkmale gleichzeitig vorliegen, gilt das Kriminalitätsrisiko als besonders hoch.“⁹³

Auf der Website wird zwischen Risk Terrain Modelling und Methoden zur Vorhersage von „Hotspots“ für Straftaten unterschieden:

„Hotspots zeigen, wo sich Straftaten häufen, aber nicht unbedingt, warum. Allzu oft konzentriert man sich auf Hotspots, ohne die räumlichen Eigenschaften zu berücksichtigen, die diese Gebiete überhaupt erst zu einem attraktiven Gebiet machen... Hotspots sind lediglich Anzeichen und Symptome für Orte, die besonders anfällig für Kriminalität sind. RTM verbessert dies durch die Bereitstellung einer räumlichen Diagnose.“⁹⁴

Risk Terrain Modelling wird derzeit in Zennevallei (Belgien) und Paris (Frankreich) eingesetzt. Die *Direction de la Sécurité de Proximité de l'Agglomération Parisienne* (DSPAP, Abteilung für lokale Sicherheit der Region Paris) begann mit der Nutzung des Algorithmus, nachdem ein Geostatistiker des ehemaligen *Observatoire National de la Délinquance et des Réponses Pénales* (ONDRP, Nationales Observatorium für Kriminalität und strafrechtliche Reaktionen)⁹⁵ mehrere Jahre mit der Rutgers University zusammengearbeitet hatte. Er erklärte:

„Ich verwende den RTM-Algorithmus (Risk Terrain Modelling) seit über acht Jahren. Er ist jetzt eine Webanwendung und viel leistungsfähiger als zuvor, basiert aber auf demselben Prinzip: Er steht im Einklang mit der situativen Kriminalprävention. Das heißt, wir identifizieren die Elemente in Kontext und Umgebung, die Kriminalität begünstigen. Indem wir also eine Umgebung analysieren und die risikoerhöhenden Faktoren identifizieren, können wir vorhersagen, was in einer ähnlichen Umgebung passieren könnte.“⁹⁶

In Zennevallei wird er für ähnliche Zwecke eingesetzt. Hier wurde das Programm von Anneleen Rummens, einer Doktorandin der Universität Gent, unter der Aufsicht des Kriminologieprofessors Wim Hardyns geleitet.⁹⁷

Es gibt weitere Systeme zur Vorhersage von Umgebungsrisiken, die den Risk-Terrain-Modelling-Algorithmus nicht verwenden. Dazu gehören MapRevelation und das „Vorhersagemodul“ des Smart-Police-Systems in Frankreich. MapRevelation war eines der ersten Systeme zum Predictive Policing, in Frankreich. Es wird von der Firma Sûreté Globale vertrieben⁹⁸ und von lokalen Behörden und Stadtpolizeien in Montpellier, Lyon, Lille, Villeurbanne, Montauban, Angers, Colombes und Melun Val de Seine eingesetzt.⁹⁹

Genutzte Daten

Das Risk-Terrain-Modelling-System nutzt verschiedene Gewichtungsfaktoren, die in das endgültige Modell einfließen. Diese Faktoren können je nach Anwendungsfall des Modells angepasst werden. Der Algorithmus weist Orten einen Anfälligkeitswert zu, der auf räumlichen Faktoren basiert, darunter:

- ob der Ort gut beleuchtet ist,
- U-Bahn- oder Bushaltestellen,
- Café-Sitzbereiche im Freien,
- Fast-Food-Restaurants,
- öffentliche Toiletten,
- Apotheken,
- Lebensmittelgeschäfte,
- Bars,
- Bäume und Bänke,
- bestimmte Arten von Geschäften,
- Schulen,
- Postämter.

Auf der Website von Risk Terrain Modelling finden sich Beispiele für weitere Faktoren wie beispielsweise: „Drogen“, „leerstehend“ und „Gangs“.¹⁰⁰

In Paris greift das Risk-Terrain-Modelling-System auf Daten der Software zum Schreiben von Verfahren der *Police*

Nationale (LRPPN, *Logiciel de Rédaction des Procédures de la Police Nationale*) zurück. Es leitet Zusammenhänge zwischen Straftaten und sogenannten Umgebungsfaktoren ab. Jean-Luc Besson, Leiter der geostatistischen Abteilung des ONDRP, gab 2018 einen Einblick in die möglichen Faktoren des Pariser Modells:

„Wenn wir uns Taschendiebstähle in der Nähe von Geldautomaten ansehen, fragen wir uns: Sind die am häufigsten betroffenen Geldautomaten rund um



*die Uhr geöffnet? Befinden sie sich in der Nähe einer Kreuzung oder eines Bahnhofs usw.?*¹⁰¹

Die Forschenden konnten nicht alle der in den Systemen zum Risk Terrain Modelling von Paris und Zennevallei verwendeten Variablen präzise ermitteln. Es ist jedoch bekannt, dass das Modell Zennevallei Faktoren wie die Wetterbedingungen während bestimmter Ereignisse berücksichtigt.¹⁰²

In Frankreich wurde MapRevelation angeblich anhand einer Terrorismusdatenbank trainiert, um Anschläge vorherzusagen.¹⁰³ Das System wird außerdem mit Daten der städtischen Polizeikräfte gespeist, die es nutzen.

Das vom französischen Unternehmen Edicia entwickelte „Vorhersagemodul“ Smart Police nutzt Techniken des maschinellen Lernens. Es stützt sich sowohl auf operative Polizeidaten (z. B. Berichte, Straftaten, Standorte von Beamten und Fahrzeugen) als auch auf städtische Daten (z. B. Umgebungs- und Wetterdaten, nationale und lokale Ereignisse, soziodemografische Daten und Wahldaten).

Das „Vorhersagemodul“ Smart Police greift angeblich auch auf Informationen aus sozialen Medien und von anderen Partnern zurück. Dazu gehören Leiter*innen von Oberschulen und Vermieter*innen von Sozialwohnungen sowie Informationen aus erster Hand von Polizeikräften.¹⁰⁴ Dies birgt offensichtlich das Risiko, dass Gerüchte, Hörensagen und ungeprüfte Meinungen in algorithmische Systeme einfließen und ihnen den Anschein technischer Objektivität verleihen.

Ergebnisse

Eine Kultur der Geheimhaltung bei Polizeikräften und Regierungsbehörden erschwerte es, schlüssige Informationen über die Ergebnisse der in Belgien und Frankreich eingesetzten Systeme zur Vorhersage von Umgebungsrisiken zu finden.

Einer von *La Quadrature du Net* kontaktierten Quelle zufolge gibt es keine schlüssigen Beweise dafür, dass das in Frankreich eingesetzte System zum Risk Terrain Modelling die Kriminalitätsrate senkt. Die Quelle gab außerdem an, dass die Methodik des Risk Terrain Modelling es Institutionen ermöglicht, sich dem Nachdenken über die strukturellen Ursachen von Kriminalität zu entziehen.¹⁰⁵ Ein ähnliches Problem ergibt sich bei anderen Systemen zur Vorhersage von „Hotspots“ für Straftaten.

Weitere standortbezogene Systeme zur Kriminalitätsvorhersage in Europa

Zusätzlich zu den oben beschriebenen Systemen in Belgien, Frankreich, Deutschland und Spanien setzen auch andere Polizeibehörden in ganz Europa Systeme zum standortbezogenen Predictive Policing ein.

Im Vereinigten Königreich stellte *Amnesty International UK* kürzlich fest, dass fast drei Viertel der Polizeibehörden Systeme zum Predictive Policing einsetzen, wobei 32 von 46 Polizeibehörden standortbezogene Systeme zur Kriminalitätsvorhersage einsetzen.¹⁰⁶ *Amnesty International* untersuchte den Einsatz von Risk Terrain Modelling durch britische Polizeibehörden und stellte fest, dass der Einsatz von Risk Terrain Modelling durch die Londoner Metropolitan Police „zu Racial Profiling und diskriminierender Polizeiarbeit beiträgt und diese verstärkt“. ¹⁰⁷ Demografische Analysen der vom Risk-Terrain-Modelling-Algorithmus als „Hochrisikogebiete“ eingestuften Gebiete zeigten:

„...die Gebiete, in denen das Risk-Terrain-Modelling-System schwere Gewalt vorhersagte, entsprechen deutlich den Gebieten mit einem höheren Anteil benachteiligter schwarzafrikanischer, schwarzkaribischer, asiatischer, bangladeschischer und asiatisch-pakistanischer Einwohner.“¹⁰⁸

Dr. Adam Elliott-Cooper, Wissenschaftler und Autor des Buches *Black Resistance to British Policing*, äußerte sich zur Verwendung umgebungsbezogener „Risikofaktoren“ zur „Vorhersage“ von Kriminalität:

„Es dürfte uns nicht überraschen, dass in den von der Polizei ins Visier genommenen bebauten Umgebungen keine Doppelhaushälften mit gepflegten Vorgärten zu finden sind. Es handelt sich um Sozialwohnungen, innerstädtische Gebiete, die im Übermaß polizeilich überwacht werden, keine wohlhabenden Vororte, oder? Wir sehen also, wie dieser vermeintlich geografische und damit vermeintlich wissenschaftlichere und objektivere Ansatz der Polizeiarbeit in Wirklichkeit lediglich diese bestehenden Probleme reproduziert.“¹⁰⁹

In den Niederlanden setzt die Polizei das „Crime Anticipation System“ ein. Dieses System zur Vorhersage von „Hotspots“ basierte ursprünglich auf Datenpunkten, beispielsweise der Anzahl „nicht westlicher“ Personen mit mindestens einem im Ausland geborenen Elternteil in einem Gebiet. Obwohl diese Datenpunkte später entfernt wurden, verwendet das System immer noch historische Kriminalitätsdaten und Proxys für Rasse und Klasse, wie beispielsweise Einkommens- und Sozialleistungsdaten.¹¹⁰

Die italienische Polizei nutzte zuvor „Delia“, ein System des Unternehmens KeyCrime.

Dieses System bietet sowohl Funktionen zur geografischen als auch zur individuellen Kriminalitätsvorhersage. Es handelt sich angeblich um eines der ersten Beispiele für kommerziell erhältliche Predictive-Policing-Software weltweit. Sie wurde bereits 2008 in Betrieb genommen.¹¹¹ KeyCrime befindet sich jedoch inzwischen in Liquidation. Als Gründe werden die finanzielle Unsicherheit durch die Einführung der KI-Verordnung der EU und die Möglichkeit eines künftigen Verbots des Systems genannt.¹¹²

In Italien wird jedoch weiterhin ein System namens XLAW eingesetzt.¹¹³ XLAW ist ein System zur Vorhersage von Umgebungsrisiken – ähnlich den in Frankreich, Belgien und dem Vereinigten Königreich eingesetzten Systemen zum Risk Terrain Modelling. Zu den räumlich-zeitlichen Prädiktoren des Systems gehören: große Veranstaltungsorte, Rentenzahlungen am Monatsende, Ladenschlusszeiten, Zug- und Schiffsankünfte sowie Wetterschwankungen.¹¹⁴

In einigen Kantonen der Schweiz setzt die Polizei PRECOBS ein – dasselbe System, das auch in Deutschland verwendet wird.¹¹⁵





Personenbezogene Systeme zur Vorhersage und zum Profiling

Personenbezogene Instrumente zur Kriminalitätsvorhersage sollen die Wahrscheinlichkeit bzw. das Risiko vorhersagen, dass eine Person bestimmte Handlungen begeht, insbesondere solche, die gesetzlich als Straftaten definiert sind. Anstatt sich auf einen bestimmten Ort zu konzentrieren, konzentrieren sie sich auf bestimmte Personen.

Polizei und Strafjustiz nutzen diese Systeme, um das Risiko einer Person, eine Straftat zu begehen oder kriminelles Verhalten zu zeigen, zu profilieren, vorherzusagen oder zu bewerten. Andere derartige Systeme versuchen die Wahrscheinlichkeit einzuschätzen, dass eine Person Opfer einer Straftat, beispielsweise geschlechtsspezifischer Gewalt, wird. Sie wurden auch eingesetzt, um mutmaßlich falsche Anzeigen aufzudecken.

Die von diesen Systemen erfassten Personen werden einer Analyse von Daten unterzogen, die sie, ihr vergangenes und gegenwärtiges Leben sowie ihre Beziehungen charakterisieren. Ziel ist es, ihr Verhalten, ihr „Risiko“ oder ihre vermeintliche „Kriminalität“ zu bestimmen und „vorherzusagen“.

Dies kann potenziell schwerwiegende Folgen haben. Diese Systeme können zur Folge haben, dass Personen überwacht oder beobachtet werden. Sie können vermehrt Polizeikontrollen, Verhören, Durchsuchungen, Haus- oder Arbeitsplatzbesuchen ausgesetzt sein. Der Einsatz dieser Systeme kann sogar zu Inhaftierung, Verhaftung oder Abschiebung führen.

Diese Systeme werden auch im Strafrechtssystem eingesetzt. Sie können die Entscheidungsfindung von Richtern beeinflussen, beispielsweise bei der Urteilsverkündung. Sie können die Dauer der Haftstrafe, den Zeitpunkt der Entlassung und die Haftbedingungen beeinflussen.

Zweck

Systeme zur personenbezogenen Vorhersage, Profiling und Risikobewertung werden für eine Vielzahl unterschiedlicher Zwecke eingesetzt. Einige Polizeikräfte nutzen Data-Mining- und Analysesoftware, um Daten zu sammeln und zu vergleichen, Muster zu bewerten und diese zur Vorhersage zukünftiger Muster zu nutzen.

In Deutschland besitzen drei Bundesländer Lizenzen für Big-Data-Mining- und Analyseprogramme, die auf der Gotham-Software des US-Technologieunternehmens Palantir basieren. Wie viele andere Unternehmen, die Polizeitechnologie entwickeln und vertreiben, ist Palantir hinsichtlich der Technologie und der unterzeichneten Verträge äußerst verschwiegen.

Die hessische Landespolizei nutzt das von Palantir betriebene System *hessenDATA* um umfassende individuelle Profile von Personen zu erstellen. Das System kann bekannte Informationen über eine Person anzeigen, darunter: wann und wo sie von der Polizei angehalten wurde, Aufzeichnungen über Festnahmen, ob sie jemals mit Drogen erwischt wurde und wo sie wohnt.

In Belgien verfügt das von der belgischen Nationalpolizei genutzte System „i-Police“ über mehrere Funktionen, darunter:

- Analyse und Vorhersage von Mustern;
- Vorhersage zukünftiger Straftaten zum Zwecke der Prävention;
- Ermöglichung von Überwachung und Beobachtung;
- Einteilung von Polizeistreifen, Kontrollen und Überprüfungen
- sowie andere Formen der Intervention und Durchsetzung.¹¹⁶

Die belgische Polizei erstellt außerdem Profile von Personen und Gruppen und erfasst diese in speziellen Datenbanken. Dieses Thema wird weiter unten ausführlicher behandelt. Dazu gehört auch die Nutzung dieser Datenbanken für sogenannte „urbane Gangs“, ein rassistisch aufgeladener Begriff.¹¹⁷ Personen, die als mutmaßliche „Gangmitglieder“ identifiziert wurden, werden gezielt überwacht, beobachtet und verstärkt angehalten und durchsucht.¹¹⁸

In Deutschland wurden individuelle Vorhersage-, Profiling- und Risikobewertungsinstrumente eingeführt, um das mutmaßliche zukünftige Risiko

durch sogenannte islamistische¹¹⁹ Terroristen oder Unterstützer des Terrorismus zu bewerten. Das Bundeskriminalamt hat mit RADAR (Rule-based Analysis of Potentially Destructive Offenders for the Assessment of Acute Risk) zwei individuelle Instrumente zur Risikobewertung entwickelt.

Eine Version, RADAR-iTE, dient der Analyse und Profilerstellung sogenannter „Islamisten“. Auch die belgische Bundespolizei gibt an, ein ähnliches Tool wie RADAR-iTE zu verwenden.¹²⁰ Das andere Instrument, RADAR-rechts, wird vom deutschen Bundeskriminalamt eingesetzt, um Profile von Personen mit rechtsextremen Ansichten zu erstellen, die als gewalttätige Bedrohung gelten. Das Amt entwickelt außerdem ein weiteres Tool, RADAR-Haft, um die Gewaltbereitschaft von Inhaftierten nach ihrer Entlassung zu bewerten.

RADAR-iTE und RADAR-rechts sollen vor allem das Risiko von Personen bewerten, die zuvor als „Gefährder“ identifiziert wurden. Diese Bedrohungsklassifizierung wurde von deutschen Strafverfolgungsbehörden entwickelt und mittlerweile in der gesamten EU übernommen.¹²¹ Der Begriff ist unklar und lässt subjektive Interpretationen zu. Die Systeme werden auch zur Bewertung „relevanter Personen“ eingesetzt, einer weiteren unklaren und subjektiven Kategorie. Die Risikoprofilerstellung dient der Bewertung und Priorisierung von Personen „mit hohem Risiko“ für spätere Strafverfolgungs- und Interventionsmaßnahmen.¹²²

In Spanien ist VioGén eines der bekanntesten Systeme zur individuellen Risikobewertung. Sein Zweck ist die Bewertung des Risikos geschlechtsspezifischer Gewalt für eine Person, die einen Vorfall gemeldet hat. Die Bewertung bestimmt die daraufhin ergriffenen Maßnahmen der Polizei.¹²³

Die spanische Polizei setzt auch ein ungewöhnlicheres Vorhersagesystem ein. VeriPol ist ein algorithmisches System, das von der spanischen Nationalpolizei eingesetzt wird, um vermeintlich falsche Anzeigen aufzudecken. Es nutzt Techniken der Verarbeitung natürlicher Sprache, um die Texte von Anzeigen über Raub, Taschendiebstahl und Handtaschenraub zu scannen. Es wird effektiv als Lügendetektor eingesetzt. Es wurde entwickelt, um Betrug durch Falschanzeigen zu verhindern. Das Hauptziel besteht darin, den Beamten eine schnelle Einschätzung zu ermöglichen, ob eine Anzeige möglicherweise falsch ist.¹²⁴ Im März 2025 wurde berichtet, dass die Nationalpolizei VeriPol mittlerweile nicht mehr nutzt. Das spanische Innenministerium begründete dies mit der mangelnden Gültigkeit des Systems in Gerichtsverfahren.¹²⁵

Sicherheitsbehörden weltweit, auch in Europa, analysieren zunehmend sogenannte „Fluggastdatensätze“ (Passenger Name Records, PNR). Dabei handelt es sich um personenbezogene Daten, die von Fluggesellschaften zu Geschäftszwecken erhoben werden, wenn eine Person einen Flug bucht.¹²⁶ PNR-Daten werden mit polizeilichen und anderen staatlichen Datenbanken abgeglichen. Diese Daten werden anhand vorgegebener

Kriterien mithilfe von Algorithmen systematisch nach Mustern durchsucht.¹²⁷ Solche Systeme stellen die Unschuldsvermutung praktisch auf den Kopf und machen alle Flugreisenden verdächtig.¹²⁸ Die EU plant, ihren Einsatz auf andere Verkehrsmittel auszuweiten, beginnend mit dem Seeverkehr.¹²⁹

In spanischen Gefängnissen wird ein System namens DRAVY eingesetzt, um Gefangene zu identifizieren, die sich mutmaßlich in einem Prozess der sogenannten „dschihadistischen“ Radikalisierung befinden.¹³⁰ Da DRAVY in erster Linie der Bewertung „dschihadistischer“ Radikalisierung dient, ist es grundsätzlich diskriminierend, da es sich fast ausschließlich auf Muslime und Personen mit muslimischem Hintergrund konzentriert. Das System zielt auf den Begriff „Dschihadismus“ ab, der selbst auf diskriminierenden westlichen Stereotypen beruht.

Ein ähnliches Instrument namens RisCanvi wird auch in spanischen Gefängnissen eingesetzt, um das Rückfallrisiko von Personen vorherzusagen. Es dient der Entscheidungsfindung über Bewährung, vorübergehende Entlassung und die Kategorisierung von Gefangenen.¹³¹

Genutzte Daten

Diese Systeme werden anhand von Daten von Polizei, Strafverfolgungsbehörden und Strafjustizbehörden trainiert, entwickelt und betrieben.

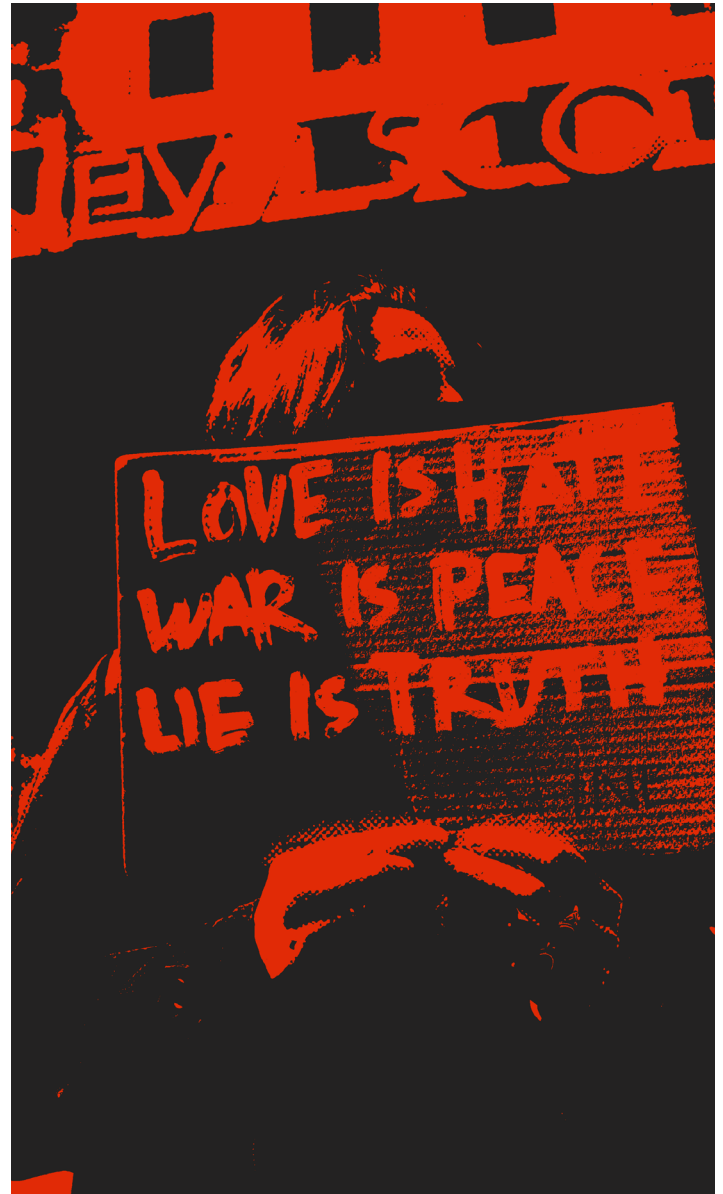
Diese Behörden erfassen oder greifen häufig auf Daten aus einer Vielzahl von Quellen zu. In Deutschland nutzen die Systeme von Palantir Daten aus Polizeidatenbanken und anderen Quellen, darunter auch soziale Medien. In den letzten Jahren wurden sowohl gegen die Systeme als auch gegen die ihrer Nutzung zugrunde liegenden Gesetze zur Datenanalyse rechtliche Schritte eingeleitet.¹³² Nachdem eine Klage erfolgreich den Umfang der Analysen und Datenquellen eingeschränkt hatte, ließ eine deutsche Polizeiquelle verlauten: „Als das Urteil verkündet wurde, gab es ein Aufstöhnen, und die Kollegen erkannten, dass ihnen so vieles nicht mehr erlaubt war.“¹³³

Das belgische System i-Police soll Daten aus allen belgischen Polizeidatenbanken und Videoüberwachungsmaterial beinhalten. Es nutzt außerdem Open-Source-Informationen wie Informationen aus den sozialen Medien und Presseberichte. Um diese Aufgaben zu erfüllen, setzt i-Police digitale Technologien verschiedener Subunternehmer ein, u. a. auch von israelischen Unternehmen wie Interionet und TA9/Rayzone. Der CEO des letzteren war früher stellvertretender Direktor der Einheit 8200, der Geheimdiensteinheit des israelischen Militärs, die für die Entwicklung und den Einsatz von „Gospel“ verantwortlich ist, einem KI-System zur automatischen Generierung von Bombenzielen im Gazastreifen im Rahmen des anhaltenden Völkermords und der Massentötung von Palästinensern durch Israel.¹³⁴

Die von diesen Systemen verwendeten Daten sind grundsätzlich verzerrt. Die Polizei in ganz Europa nimmt überproportional Personen aus ethnischen Minderheiten ins

Visier. In Spanien werden von der Polizei beispielsweise überproportional viele Personen aufgrund ihrer rassistischen, ethnischen oder religiösen Herkunft angehalten und durchsucht.¹³⁵ In Deutschland sind Personen mit nichtdeutscher Staatsangehörigkeit unter den von der Polizei erfassten Verdächtigen, den von Gerichten Verurteilten und den Inhaftierten überrepräsentiert.¹³⁶ Das belgische Strafrechtssystem wurde bereits mehrfach für seine rassistischen Praktiken, insbesondere für Ethnic Profiling, verurteilt.¹³⁷ Der UN-Ausschuss für die Beseitigung der Rassendiskriminierung (CERD) äußerte seine Besorgnis darüber, dass Menschen mit ausländischem Hintergrund im belgischen Strafrechtssystem, insbesondere im Gefängnis, überrepräsentiert sind.¹³⁸

Die in diesen digitalen Systemen verwendeten Daten der Polizei und des Strafrechtssystems sind voll von strukturellen und institutionellen Verzerrungen, Überrepräsentationen und Diskriminierung. Dennoch werden sie genutzt, um datenbasierte Systeme zur Vorhersage, zum Profiling und zur Risikobewertung zu entwickeln und zu betreiben. Dies führt zu einem verstärkten Fokus auf dieselben marginalisierten Gruppen und Gemeinschaften. Die Ergebnisse dieser Vorgänge fließen dann zurück in die Systeme, wodurch die Wahrscheinlichkeit steigt, dass Personen aus diesen Gruppen und Gemeinschaften in Zukunft als „hochriskant“ eingestuft werden. Auf diese Weise erzeugen diese Algorithmen eine sich selbst erfüllende Prophezeiung bzw. eine Rückkopplungsschleife. Es gibt klare Beispiele dafür, wie diese diskriminierenden Daten die Ergebnisse dieser Systeme beeinflussen.



Die vollständige Liste der vom deutschen Profiling-System RADAR-iTE verwendeten Daten ist nicht bekannt. Es basiert jedoch auf einer Fernbewertung ohne direkten Kontakt mit der zu bewertenden Person.¹³⁹ Die Bewertung umfasst Themen wie „Gewalt gegen Personen“, „Interaktion mit Behörden und anderen Institutionen“ sowie „Militär und Reisen“. Weitere Fragen lauten beispielsweise: „Wie sieht das Privatleben der Person aus? Ist sie eher ein Einzelgänger oder agiert sie in einer Gruppe? Hat sie Kontakte außerhalb der

islamistischen Szene? Hat sie Arbeit?“¹⁴⁰

Solche Profiling-Punkte bedeuten, dass eine Person, die aus einem Konfliktgebiet angereist ist oder bestimmte Routen für Tourismus oder Familienbesuche nutzt, als verdächtig oder als „Risiko“ eingestuft werden kann. Datenpunkte wie Bekannte, Kontakte oder Reismuster können eindeutig zu Diskriminierung führen.¹⁴¹ Die Bewertung von RADAR-iTE enthält auch weitere besorgniserregende und potenziell diskriminierende Informationen zu psychischen Erkrankungen und Suizidalität.¹⁴²

Darüber hinaus gab es Probleme mit den Daten, die zum Training des inzwischen abgeschafften spanischen Systems VeriPol verwendet wurden, das zur Erkennung falscher Anzeigen eingesetzt wurde. VeriPol wurde anhand von Anzeigen trainiert, die der Polizei vorgelegt und von Beamt*innen manuell als falsch oder echt katalogisiert wurden. Da jedoch nicht alle dieser Fälle aufgeklärt wurden, gab es keine objektive oder schlüssige Feststellung von Wahrheit oder Falschheit. Das Modell basierte daher ausschließlich auf den Annahmen der Polizeikraft, die diese Anzeigen katalogisierte.¹⁴³ Es ist bemerkenswert, dass die spanischen Behörden mindestens sieben Jahre brauchten, um die Probleme des Systems zu erkennen und dessen Nutzung einzustellen.

Mit dem in Spanien eingesetzten System VioGén kann angeblich vorhergesagt werden, ob jemand geschlechtsspezifische Gewalt erfahren wird. Das System nutzte jedoch nicht die tatsächlichen Aussagen der Frauen, die Fälle geschlechtsspezifischer Gewalt meldeten, sondern die Berichte der Polizeikräfte über die Berichte der Frauen. Der resultierende Risikowert hängt daher vollständig von der Einschätzung der Polizeikraft ab.¹⁴⁴ Das System kann zudem nur Daten aus tatsächlich eingereichten Anzeigen verarbeiten.

Viele Erfahrungen geschlechtsspezifischer Gewalt werden jedoch nicht gemeldet, insbesondere die von Migrantinnen, Frauen aus marginalisierten und sozial schwachen Verhältnissen sowie Frauen mit Kindern. Neben LGBTQIA+-Personen und Menschen mit Behinderungen sind diese Gruppen am stärksten von strukturellen Schwierigkeiten beim Anzeigen ihrer Aggressoren betroffen. Das System berücksichtigte daher die Erfahrungen der am stärksten marginalisierten Menschen in der Gesellschaft nicht vollständig.¹⁴⁵

Die Konzepte, die diesen Systemen zur Vorhersage, zum Profiling und zur Risikobewertung zugrunde liegen, sind zudem grundsätzlich von Vorurteilen beeinflusst. Dieses Problem resultiert aus mangelnder Klarheit, die zu Subjektivität führt, oder aus kulturspezifischen Begriffen mit rassifizierten Untertönen.

In Deutschland werden vage Begriffe wie „Gefährder“ und „relevante Person“ verwendet, um Personen zu kategorisieren, die verdächtig werden, Gewalt auszuüben oder befürworten. Sie haben sich bei Sicherheitsbehörden und der Polizei als Arbeitsbegriffe etabliert und werden in den RADAR-Systemen verwendet. Sie sind gesetzlich nicht

definiert, vage und unwissenschaftlich. Das bedeutet, dass Personenprofile subjektiv, nach Ermessen der Behörden und uneinheitlich erstellt werden. Das untergräbt die gesamte Legitimität des Systems.

Diese Probleme werden durch die praktische Verwendung der Begriffe offengelegt. Die deutschen Polizeibehörden waren deutlich zögerlicher, Rechtsextremisten als gefährlich einzustufen als sogenannte „Islamisten“. So waren beispielsweise bei der Aufdeckung der terroristischen Neonazi-Organisation NSU (Nationalsozialistischer Untergrund) im Jahr 2011 nur vier Mitglieder der Gruppe als „Gefährder“ eingestuft worden.¹⁴⁶

Mit den in diesen Systemen verwendeten Daten gibt es noch weitere Probleme. Das belgische System i-Police führt Daten aus verschiedenen polizeilichen Quellen zusammen, darunter auch „nicht validierte“ Informationen. Dazu gehören unbestätigte Informationen aus Polizeiberichten, die oft als polizeiliche „Informationen“ bezeichnet werden und Informationen über Personen enthalten, die in Bezug auf Straftaten weder verurteilt noch angeklagt wurden. Der Vorsitzende der Datenschutzbehörde COC, die die belgische Polizei beaufsichtigt, hat hinsichtlich der Verwendung dieser Daten im System i-Police ernsthafte Bedenken geäußert.¹⁴⁷

Systeme, die potenzielle Kriminalität, zukünftige Kriminalität oder das „Risiko“ von Kriminalität bewerten, stellen einen konzeptionellen Wandel dar, von Bewertungen, die auf tatsächlichen Beweisen einer Handlung oder Beteiligung an einer Handlung basieren, hin zu



einem unbestimmten, abstrakten Risiko, das sich in der Zukunft entwickeln könnte und oft nur auf der Grundlage von Indizien abgeschätzt wird. Das gilt für alle individuellen oder personenbezogenen Systeme.

Ergebnisse und Auswirkungen

Diese Systeme zur Vorhersage, zum Profiling und zur Risikobewertung werden eingesetzt, um eine Reihe von Entscheidungen und Ergebnissen der Polizei und Strafverfolgung zu beeinflussen, von Überwachung und Beobachtung über Kontrollen und Befragungen, Durchsuchungen und Hausdurchsuchungen bis hin zu Festnahmen.

Das hessische Polizeisystem hessenDATA ermöglicht eine äußerst invasive Überwachung. Trotz seiner angeblichen Verwendung für „schwere“, „organisierte“ oder „staatsgefährdende“ Kriminalität wird es in großem Umfang für gewaltlose Straftaten eingesetzt. Im Jahr 2022 wurde berichtet, dass die Polizei rund 12.000 der jährlich 14.000 Abfragen im System hessenDATA als „Präventionsmaßnahmen“ gegen Straftaten einstufte.¹⁴⁸

Die Ergebnisse dieser Systeme ordnen Personen in der Regel einen Risikowert zu: niedrig, mittel oder hoch bzw. Variationen dieser Kategorien. Dies gibt Aufschluss über die vermeintliche Wahrscheinlichkeit, eine Straftat zu begehen oder kriminelles Verhalten zu zeigen.

Laut dem Bundeskriminalamt wurden seit 2017 rund 800 Personen aus dem „islamistischen“ Spektrum von RADAR-iTE bewertet.¹⁴⁹ Bis November 2023 wurden 487 Personen in Zusammenhang mit „politisch motivierter“ Kriminalität mit religiöser Ideologie als „Gefährder“ eingestuft. Im Gegensatz dazu ist die Zahl der als „Gefährder“ oder „relevante Personen“ eingestuften rechtsextremen Personen – ebenso wie die Zahl der RADAR-rechts-Bewertungen.¹⁵⁰

Das von der spanischen Polizei verwendete System VioGén dient zur Vergabe von Risikobewertungen, allerdings für Opfer anstatt für Täter. Ein niedriger Wert bedeutet, dass die Polizei das Opfer beispielsweise telefonisch kontaktiert, während ein extremer Risikowert bedeuten kann, dass die Polizei die Wohnung des Opfers überwacht oder Sicherheitspatrouillen einsetzt, um dessen Sicherheit zu gewährleisten.¹⁵¹ In 95 % aller Fälle folgen die Polizeikräfte dem von VioGén ausgegebenen Risikowert und den dafür geltenden Empfehlungen.¹⁵²

Aufgrund von Profiling anhand von Fluggastdatensätzen (PNR) stufte das Bundeskriminalamt Routen zwischen der Türkei und Deutschland als potenziell verdächtig ein. Sie werden angeblich häufig von „islamistischen“ Terroristen genutzt, „da sie auch bei Touristen beliebt sind und daher günstige Preise und gute Tarnmöglichkeiten bieten“.¹⁵³

Das in spanischen Gefängnissen eingesetzte System DRAVY prognostiziert für fast die Hälfte der untersuchten Personen fälschlicherweise ein hohes Risiko.¹⁵⁴ Dies führt zu

einer strengeren Behandlung und härteren Lebensbedingungen im Gefängnis. Nichtspanische Staatsangehörige sind überproportional betroffen.¹⁵⁵ Das System RisCanvi, das auch in Spanien eingesetzt wird, diskriminiert bekanntermaßen aufgrund des sozioökonomischen Status oder der Zugehörigkeit zu anderen Personen. Es vergibt höhere Risikobewertungen für Personen mit einer Vorgeschichte „instabiler“ Beschäftigungs- und Finanzsituationen, Personen ohne familiäre oder soziale Unterstützung sowie Personen mit kriminellen Familienmitgliedern oder Eltern.¹⁵⁶



Bis September 2023 wurden im System VioGén rund 770.000 Fälle ausgewertet.¹⁵⁷ Systeme zur Erfassung von Fluggastdatensätzen (PNR-Systeme) erstellen Profile von Millionen von Fluggästen. Im Jahr 2022 übermittelten 156 Fluggesellschaften in Deutschland an die Polizei rund 424 Millionen PNR-Datensätze von rund 121 Millionen Passagieren. Im Jahr 2023 wurden bis zum 31. Oktober rund 385 Millionen PNR-Datensätze zu 107 Millionen Passagieren generiert.

Menschen, sondern haben auch dazu geführt, dass eine beträchtliche Zahl von Menschen polizeilichen Eingriffen ausgesetzt war. Im Jahr 2023 ergriff die deutsche Polizei auf der Grundlage von PNR-Profiling mehr als 10.000 Maßnahmen. Fast ein Fünftel davon erwiesen sich als falsch positive Ergebnisse (falsche Übereinstimmungen).¹⁵⁸ In den 8.284 Fällen richtig positiver Ergebnisse (richtige Übereinstimmungen) wurden die folgenden Maßnahmen ergriffen:

- 2.178 Überprüfungen des Aufenthaltsstatus;
- 2.394 polizeiliche Beobachtungen/verdeckte Kontrollen;
- 1.236 Festnahmen, 2.303 gezielte (offene) Kontrollen und
- 173 Zurückweisungen/Einreiseverweigerungen.¹⁵⁹

Millionen von Passagierdatensätzen werden so analysiert, um mehrere Tausend straf- oder einwanderungsrechtliche Ermittlungen durchzuführen, deren objektive Beweisgrundlage nicht vorhanden oder äußerst dürftig ist.

Einzelne im Bericht über Deutschland hervorgehobene Fälle verdeutlichen, welche extremen Folgen es haben kann, wenn man (fälschlicherweise) als „Gefährder“ bezeichnet wird. Antimuslimische Vorurteile führen dazu, dass die Polizei und Behörden muslimische Jugendliche anders behandeln als weiße junge Männer mit ähnlichem problematischem Verhalten, sodass sie schneller als Bedrohung angesehen werden.¹⁶⁰

Die Folgen einer Profilerstellung durch das System RADAR-iTE sind u. a.:

- Beobachtung und Überwachung;¹⁶¹
- „Präventivhaft“ von mehreren Tagen bis zu Monaten;¹⁶²
- Inhaftierung vor der Abschiebung¹⁶³ und anschließende Abschiebung.¹⁶⁴

Auch Asylanträge von Personen, die einem Profiling unterzogen werden, können ausgesetzt werden.¹⁶⁵

Weitere personenbezogene Systeme zur Kriminalitätsvorhersage in Europa

Neben den oben genannten Beispielen setzen auch in anderen europäischen Ländern Polizei und Strafverfolgungsbehörden personenbezogene Instrumente zur Kriminalitätsvorhersage und zum Profiling ein. Frühere Untersuchungen ergaben Hinweise auf ähnliche Systeme bei Polizeikräften und Gefängnissen im Vereinigten Königreich, in Italien und in den Niederlanden.

Amnesty International UK gab kürzlich bekannt, dass elf Polizeikräfte im Vereinigten Königreich personenbezogene oder individuelle Instrumente zur Kriminalitätsvorhersage und zum Profiling einsetzten.¹⁶⁶ Dazu gehören:

- Das „Violence Harm Assessment“ der London Metropolitan Police, das Personen in ganz London auf ihr Gewaltrisiko hin profiliert. Bis August 2024 waren 66 % der vom System erfassten Personen schwarz, während nur 22 % weiß waren;
- Das „Integrated Offender Management“-System (IOM) der West Midlands Police zur Vorhersage des Potenzials von Personen, in Zukunft Schaden anzurichten. Die interne Analyse der Polizei ergab, dass Schwarze 2,4-mal häufiger zur Gruppe mit dem höchsten vorhergesagten Potenzial, Schaden zuzufügen, gehören wie nordeuropäische (weiße) Personen.

In ganz England und Wales nutzen Gefängnisse und Bewährungshilfen das Offender Assessment System (OASys), um das Rückfallrisiko aller Personen, die in das Strafrechtssystem eintreten, vorherzusagen. Dieses System wurde weithin kritisiert, weil es rassistische Profile erstellt, die Privatsphäre bedroht und keine Möglichkeiten zur Rechenschaftslegung oder Wiedergutmachung bietet.¹⁶⁷

In den Niederlanden setzt die Polizei das System ProKid ein, das das Rückfallrisiko von Kindern und Jugendlichen vorhersagen soll.¹⁶⁸ In Amsterdam setzte die Polizei zwei Profiling-Tools namens Top400 und Top600 ein, mit denen versucht werden soll, Profile der 600 bzw. 400 Jugendlichen zu erstellen, die mutmaßlich am wahrscheinlichsten verschiedene Arten von Straftaten begehen.¹⁶⁹

Diana Sardjoe, eine Mutter, deren Söhne von Top400 und Top600 profiliert wurden, erklärte, die Systeme hätten dazu geführt, dass ihre Söhne ständig überwacht und schikaniert würden. Sie forderte ein Verbot von Predictive-Policing-Systemen.¹⁷⁰

Auch in Italien setzte die Polizei früher das Profiling-System Delia ein, das ethnische Daten zur Profilerstellung von Personen einbezog.¹⁷¹





KI-Videoüberwachungssysteme

Polizeibehörden in ganz Europa setzen zunehmend KI-Videoüberwachungssysteme ein. Diese Systeme nutzen KI-basierte Methoden, um Videomaterial, beispielsweise von Überwachungskameras und Polizeidatenbanken, zu durchsuchen, um Personen und Objekte zu identifizieren oder „verdächtiges“ Verhalten zu erkennen.

Die diesem Bericht zugrunde liegende Forschungsarbeit umfasst Beispiele für KI-Videoüberwachungssysteme, die von Polizeikräften in Belgien und Spanien eingesetzt werden. *La Quadrature du Net* hat unabhängig davon umfangreiche Untersuchungen zum polizeilichen Einsatz von KI-Videoüberwachung in Frankreich durchgeführt.¹⁷² In Deutschland identifizierte *AlgorithmWatch* zwei Pilotprojekte zur KI-Videoüberwachung zur Selbstmordprävention in Gefängnissen. Auch in Italien gibt es Hinweise auf den Einsatz von KI-Videoüberwachung durch die Polizei.

Der Einsatz von KI-Videoüberwachung durch Strafverfolgungsbehörden gibt Anlass zu erheblichen Bedenken hinsichtlich der Verletzung von Grundrechten, einschließlich des Rechts auf Privatsphäre und Nichtdiskriminierung.

Polizeiarbeit

In Spanien nutzen mehrere Madrider Kommunen Videoüberwachungssysteme mit KI-Methoden zur Bilderkennung. Die von Bosch Security über das US-amerikanische Unternehmen Intelligent Security Services bereitgestellten Systeme dienen zwei Zwecken: der automatischen Kennzeichenerkennung (ANPR) und der Identifizierung von Tatverdächtigen.¹⁷³ Das System kann auch zur Personensuche anhand von Merkmalen wie Haarfarbe, Kleidung, Gesichtszügen und Alter eingesetzt werden. Es gibt keine konkreten Belege dafür, dass das System die Kriminalitätsrate senkt.¹⁷⁴ In Madrid waren im Januar 2025 mindestens 83 KI-Überwachungskameras im Einsatz, die von der Stadtpolizei betrieben werden. Die Installation von weiteren 38 Kameras ist geplant.¹⁷⁵

In Belgien nutzen die lokalen Polizeikräfte und die Bundespolizei mehrere KI-Videoüberwachungssysteme. Dazu gehört Software des israelischen Unternehmens BriefCam zur retrospektiven Bildanalyse durch die Zusammenfassung von Videos.¹⁷⁶ Wie das Bosch-System in Spanien ermöglicht es dieses System der Polizei, Personen nach Kriterien wie Kleidungsfarbe, Geschlecht oder Eigentum zu kategorisieren.

Letzteres könnte rechtswidrig sein. Die belgischen rechtlichen Rahmenbedingungen in Bezug auf Nichtdiskriminierung gestatten gezielte Forschung auf der Grundlage objektiver Kriterien, verbieten jedoch das massenhafte Sortieren von Personen. Aufgrund dieser und anderer Beispiele fordert der belgische Bericht, die im Rahmen des riesigen Projekts i-Police geplanten KI-Videoüberwachungen fallen zu lassen.

Im Jahr 2023 legalisierte Frankreich als erstes europäisches Land im Rahmen eines Gesetzes zur Organisation der Olympischen Spiele 2024 in Paris biometrische Überwachung in Form von algorithmisch gesteuerten Videoüberwachungskameras.¹⁷⁷ Das System wurde in Saint-Denis eingesetzt, einem Vorort im Norden von Paris, indem überwiegend Angehörige von ethnischen Minderheiten und der Arbeiterklasse leben und in dem ein Großteil der Olympischen Spiele stattfand.¹⁷⁸ Das System war ursprünglich bis Ende 2024 befristet – doch unmittelbar nach den Olympischen Spielen versuchten die Behörden seine Nutzung zu verlängern.¹⁷⁹

Andernorts in Frankreich kämpft *La Quadrature du Net* seit drei Jahren juristisch gegen die Einführung der KI-gestützten Videoüberwachungssoftware Briefcam in Moirans in der Region Isère. Am 30. Januar 2025 entschied ein Gericht, dass die Nutzung dieses Systems rechtswidrig war: Sie verstoße gegen mehrere Datenschutzbestimmungen des EU-Datenschutzrechts und der französischen Rechtsvorschriften für innere Sicherheit.¹⁸⁰

Das Urteil setzt rechtliche Rahmenbedingungen außer Kraft, die automatische Videoüberwachungssysteme zuvor zugelassen hatten, darunter auch solche, die durch befristete experimentelle Genehmigungen für die Olympischen Spiele 2024 in Paris

eingeführt wurden. Das Urteil schuf zudem einen wichtigen Präzedenzfall für die laufenden Klagen gegen algorithmische Systeme, die von der französischen Polizei eingesetzt werden.¹⁸¹

Gefängnisse

In Deutschland identifizierte *AlgorithmWatch* in Gefängnissen zwei Pilotprojekte zur KI-Videoüberwachung zur Selbstmordprävention. Diese dystopischen Überwachungssysteme sollten die bestehende Videoüberwachung in Gefängniszellen um Algorithmen für maschinelles Lernen ergänzen, um frühe Anzeichen von Selbstmordversuchen zu erkennen.

In Nordrhein-Westfalen versuchten das Justizministerium und das deutsche IT-Unternehmen FusionSystems, einen Algorithmus für maschinelles Lernen zu entwickeln, der auf von Schauspieler*innen erstellten Trainingsaufnahmen basiert. Der Algorithmus wurde darauf trainiert, Objekte (z. B. Messer, Scheren, Seile, Feuerzeuge) und Verhaltensweisen zu erkennen, die auf Selbstmordabsichten hindeuten könnten. Dazu gehören beispielsweise das Formen einer Schlinge aus einem Gürtel, das Verknoten eines Seils oder das Befestigen einer Schlinge am Fenstergitter, das Ziehen eines Messers oder das Spielen mit einem großen Messer. Der Algorithmus wurde außerdem mit Aufnahmen unauffälligen Verhaltens wie Hocken, Lesen oder Fernsehen trainiert. Dadurch sollte das System lernen, zwischen harmlosen Situationen und Anzeichen von Selbstmordgefahr zu unterscheiden.¹⁸² Das System soll zudem Skelett-Tracking beinhalten, das Sensoren und maschinelles Lernen nutzt, um die Gelenk- und Körperbewegungen einer Person zu verfolgen.¹⁸³

Mithilfe dieser Faktoren soll der Situation in der Zelle eine „Gefahrenstufe“ zugeordnet werden, die ständig neu berechnet wird. Die Beamten im Gefängnis werden durch ein optisches Ampel-Alarmsystem über die aktuelle Lage informiert. Bei hoher „Gefahrenstufe“ ertönt ein akustischer Alarm, der ein schnelles Eingreifen ermöglicht.

In Niedersachsen haben das FZI Forschungszentrum Informatik und das IT-Sicherheitsunternehmen VOMATEC Innovations ein ähnliches System entwickelt. Ziel ist die Entwicklung einer prototypischen Betriebssoftware, die voraussichtlich zunächst in der JVA Oldenburg zum Einsatz kommen wird.¹⁸⁴

Das Projekt sah zunächst den Einsatz von KI-Überwachungstechnologie in Gemeinschaftsbereichen, beispielsweise im Freien oder in Freizeiträumen, vor. Dadurch sollte beispielsweise die „Weitergabe verbotener Gegenstände zwischen Gefangenen“ erkannt werden.¹⁸⁵ Dies führte jedoch zu heftiger Kritik der niedersächsischen Datenschutzbehörde.¹⁸⁶ Anders als das System in Nordrhein-Westfalen, das mit Filmmaterial von Schauspieler*innen trainiert wurde, wird das System in Niedersachsen anhand von realen Aufnahmen von Selbstmordversuchen und Gewalt in Gefängnissen trainiert.¹⁸⁷

Der Einsatz KI-basierter Systeme zur Analyse von Emotionen oder Körperbewegungen

ist mit erheblichen Bedenken verbunden. Die Technik ist nicht nur wissenschaftlich nicht belegt,¹⁸⁸ sondern auch anfällig für rassistische oder ethnische Vorurteile. Beispielsweise ist die Kameratechnik möglicherweise nur auf hellere Hauttöne kalibriert. Der Gesichtsausdruck schwarzer Männer wird eher als „aggressiv“ interpretiert als der weißer Männer.¹⁸⁹ Kulturelle Vorurteile können das normative Verständnis von Körpersprache oder Gesichtsausdruck beeinflussen. Weitere Faktoren, die diese Technik beeinflussen können, sind schlechte Beleuchtung oder durch Brillen oder Kopftücher verdeckte oder veränderte Gesichter.

Angesichts der potenziell lebensbedrohlichen Folgen falsch negativer Ergebnisse ist der zukünftige Einsatz dieser Systeme äußerst besorgniserregend. Selbst wenn sie wie vorgesehen funktionieren und eine ausreichende Genauigkeit aufweisen, sind sie hochgradig invasiv¹⁹⁰ und greifen tief in die Privatsphäre von Inhaftierten ein. Ein ehemaliger Häftling, der von *AlgorithmWatch* interviewt wurde, erklärte, dass eine wirklich wirksame Selbstmordprävention die Abschaffung des Gefängnissystems erfordern würde:

„Ein Gefängnis ist kein therapeutischer Ort; es dient nicht der Rehabilitation, sondern der Bestrafung. Daher gibt es keine Hilfe für Menschen in Not. Das ist sehr deprimierend, und ich sehe, dass die Menschen nicht lange durchhalten können... Es gibt auch andere Möglichkeiten, Selbstmord zu verhindern: durch Therapie und Empathie, gemeinschaftliche Unterstützung und Menschen dabei zu helfen, ihrem Leben einen Sinn zu geben.“¹⁹¹

In Spanien startete das Justizministerium 2023 im Gefängnis Mas d'Enric in der Nähe von Tarragona ein Pilotprojekt mit Gesichtserkennungs- und Videoanalysekameras zur „Echtzeiterkennung nonverbaler Ausdrücke und Einstellungen, die auf rechtswidriges Verhalten hindeuten“. Das teilweise von der Europäischen Union finanzierte Projekt sollte auf andere Gefängnisse in der Region ausgeweitet werden. Die katalanische Regierung kündigte jedoch im Januar 2024 an, das Projekt angesichts des kürzlich verabschiedeten KI-Gesetzes nicht weiterzuführen.¹⁹²



Datenbanken

Datenbanken liefern häufig die Daten, die in den von Polizei und Strafverfolgungsbehörden eingesetzten Systemen zur Vorhersage, zum Profiling und zur Risikobewertung verwendet werden. Sie können auch die Begründung oder vermeintliche Beweisgrundlage für polizeiliche und strafrechtliche Maßnahmen liefern. Sie decken ein breites Spektrum von Bevölkerungsgruppen ab und können eine große Menge sensibler Daten enthalten, von biografischen Daten über Fingerabdrücke und Fotos bis hin zu Vorstrafen und vielem mehr.

In Belgien gibt es verschiedene Kategorien von Datenbanken, die von Polizei und Strafverfolgungsbehörden genutzt werden:

- Die nationale allgemeine Datenbank wird für polizeiliche Ermittlungen verwendet;
- Basisdatenbanken bestehen aus Aufzeichnungen und Informationen der Polizei;
- Spezialdatenbanken werden von der Polizei für bestimmte Zwecke eingerichtet, zum Beispiel für sogenannte „urbane Gangs“;
- gemeinsame Datenbanken tauschen Daten zwischen Polizei und Geheimdiensten für mutmaßliche Terrorismuszwecke aus und
- technische Datenbanken enthalten automatisch erfasste Daten, beispielsweise von ANPR-Kameras.¹⁹³

Die französische *Police Nationale* und die *Gendarmerie* nutzen für ihre täglichen

Aktivitäten die Datenbank TAJ („Behandlung von Strafregistern“). Die französischen Behörden haben versucht, diese Datenbank mit mehreren anderen Datenbanken zu verknüpfen.¹⁹⁴ Sie enthält eine breite Palette von Informationen über Personen, die verdächtigt werden, eine schwere Straftat begangen zu haben, sowie über Opfer von Straftaten.¹⁹⁵ Bei den kommunalen französischen Polizeikräften ist die illegale Datenerfassung gängige Praxis.¹⁹⁶

Die *Police Nationale* und die *Gendarmerie* sind berechtigt, TAJ im Rahmen gerichtlicher Ermittlungen zur *nachträglichen* Gesichtserkennung zu nutzen. Das bedeutet, dass sie beispielsweise Aufnahmen aus der Videoüberwachung oder Fotos von Verdächtigen erfassen und damit die Datenbank nach übereinstimmenden Datensätzen durchsuchen können. Die Gesichtsvergleichsfunktion wird auch zunehmend für administrative Identitätsprüfungen eingesetzt. Zu diesem Zweck wird das System täglich mehr als 1.600-mal genutzt.¹⁹⁷

Die spanische Polizeidatenbank für Ausländer, ADEXTTRA, enthält eine umfangreiche Liste mit Hintergrundinformationen. Dazu gehören:

- Staatsangehörigkeit;
- Familienstand;
- Beruf und Arbeitstätigkeit;
- Eigentumsverhältnisse;
- Einkommen und Einkünfte;
- Informationen über das Zusammenleben;
- Führungszeugnisse, Haft- und außergerichtliche Inhaftierungen sowie Vorstrafen;
- Fotos und andere Bilder;
- Fingerabdrücke und
- Stimmproben.¹⁹⁸



Die von Polizei und Strafverfolgungsbehörden in Europa genutzten Datenbanken enthalten riesige Datenmengen. Die belgische nationale allgemeine Datenbank enthält Informationen über drei Millionen Menschen – ein Viertel der belgischen Bevölkerung.

In Frankreich enthält die TAJ-Datenbank fast 20 Millionen Einzeldatensätze und rund 10 Millionen Gesichtsfotos.¹⁹⁹ Die 2016 vom Innenministerium eingerichtete Datenbank *Titres électroniques sécurisés* (TES oder „sichere elektronische Dokumente“) enthält Informationen über alle Personen, die Personalausweise und Reisepässe beantragt

haben.²⁰⁰ Das französische Innenministerium könnte in Zukunft möglicherweise auf das Gesichtsbild jeder Person zugreifen können, die sich auf französischem Gebiet aufhält.²⁰¹ Dies steht im Einklang mit den Plänen der EU, „Identitätsdaten“ über jede*n einzelne*n Ausländer*in auf EU-Gebiet zu erfassen und der Polizei und den Einwanderungsbehörden zur Verfügung zu stellen.²⁰²

Hunderte französischer Polizeibehörden sind mit der Software „Smart Police“ ausgestattet. Diese Plattform und digitale Anwendung ermöglicht es ihnen, unterwegs Berichte zu erstellen, Fotos aufzunehmen und Ereignisse zu beschreiben. Die entsprechenden Daten können dann in relevante zentrale Datenbanken eingespeist werden. Smart Police umfasst eine „vorhersagende“ Komponente, die Informationen aus verschiedenen Quellen zusammenträgt. Dazu werden Kriminalitätsdaten der Polizei und Standortdaten der Beamten mit sozioökonomischen Bevölkerungsdaten, Wettervorhersagen und „Gerüchten“ von Schuldirektor*innen, Vermieter*innen und sogar aus sozialen Medien kombiniert, um das Kriminalitätsrisiko vorherzusagen.²⁰³

Die in diesen Datenbanken gespeicherten Daten und ihre Verwendung können schwerwiegende Folgen haben. Sie enthalten große Mengen falscher Informationen sowie unbestätigte Informationen, die als „Erkenntnisse“ präsentiert werden.

Ungenaue Daten mögen harmlos erscheinen, können aber schwerwiegende Folgen haben. Wenn beispielsweise veraltete Informationen über eine Person in einer Datenbank gespeichert sind, kann dies zu ihrer unrechtmäßigen Verhaftung führen. In Spanien wurden Migrant*innen fälschlicherweise inhaftiert, weil ihre Einträge in den Datenbanken nicht ordnungsgemäß aktualisiert wurden.²⁰⁴

Neben sachlich korrekten Informationen können in Systemen zur Vorhersage und zum Profiling sogenannte polizeiliche Erkenntnisse verwendet werden. Dies beeinflusst die Ergebnisse der Systeme und damit die Entscheidungen von Polizei und Strafverfolgungsbehörden. Dadurch werden unbestätigte Informationen zu Fakten verfälscht, die dann gegen Personen verwendet werden.

Datenbanken geben in Bezug auf rechtswidrige Diskriminierung Anlass zu erheblichen Bedenken. Sie können aufgrund der Herkunft und der Art der enthaltenen Daten *per se* diskriminierend sein. Ihre Nutzung kann auch zu diskriminierenden Praktiken führen.²⁰⁵ In den Datenbanken der Polizei und des Strafrechtssystems sind marginalisierte Personen, Gruppen und Gemeinschaften, die in der Vergangenheit von staatlichen Behörden ins Visier genommen, überwacht und bestraft wurden, deutlich überrepräsentiert. Dazu gehören schwarze und rassifizierte Personen und Gemeinschaften, Migrant*innen und Personen aus der Arbeiterklasse und sozioökonomisch benachteiligten Gebieten, queere Menschen und Menschen mit psychischen Erkrankungen.²⁰⁶ In mehreren deutschen Bundesländern

gibt es Datenbanken mit Bezeichnungen wie „Junkie“, „Landstreicher“, „Zigeuner“ und „ansteckend“, letzteres in Bezug auf Menschen mit HIV.²⁰⁷

Immer mehr Arbeitgeber und Behörden nutzen belgische Polizeidatenbanken für Sicherheitsüberprüfungen. Personen nordafrikanischer und belgisch-marokkanischer Herkunft sind unter denjenigen, die diese Überprüfungen nicht bestehen, überrepräsentiert. Im Bericht über Belgien wird auch die Geschichte eines jungen muslimischen Mannes erzählt, dem aufgrund fehlerhafter Angaben in einer Polizeidatenbank die Arbeitsaufnahme verweigert wurde.²⁰⁸

Die belgische Polizei ist dafür bekannt, Datenbanken einzurichten, um sogenannte „urbane Gangs“ ins Visier zu nehmen – ein Begriff, der stark von rassistischen Vorstellungen gegenüber jungen Männern geprägt ist. Die Konzeption dieser Gruppen als „urban“ und als „Gang“ ist auf ihre ethnische Zugehörigkeit zurückzuführen, und die Parameter für die Aufnahme in diese Datenbanken waren vage. Die in den Datenbanken erfassten Personen wurden gezielt überwacht, beobachtet und verstärkt angehalten und durchsucht.²⁰⁹

Die belgische Polizei führt auch Datenbanken über Prostituierte. Sie dienen angeblich der „Regulierung“ der Branche und ermöglichen die Überwachung und Verfolgung der Prostituierten. Da die Registrierung für Prostituierte obligatorisch ist, werden Personen mit irregulärem oder prekärem Migrationsstatus ausgeschlossen und von Unterstützungs- und Sicherheitsnetzwerken ferngehalten.²¹⁰

Die spanische Datenbank ADEXTTRA wird verwendet, um Migrant*innen zu identifizieren und ihren Aufenthaltsstatus im Land zu überprüfen. Es erleichtert polizeiliche Identitätskontrollen von Personen, die als „ausländisch“ angesehen werden. Es ist hinreichend belegt, dass die spanische Polizei Racial Profiling betreibt.²¹¹

Die polizeiliche Nutzung dieser Datenbanken und der darin enthaltenen Informationen unterliegt schwachen Beschränkungen und Sicherheitsvorkehrungen, deren Durchsetzung ebenso schwach ist. Polizeikräfte, die illegal auf Daten zugreifen oder gegen die Anforderungen oder Richtlinien verstoßen, werden oft weder gemeldet noch bestraft.²¹² Außerdem werden Fristen für die Aufbewahrung von Daten häufig überschritten, was dazu führt, dass personenbezogene und potenziell sensible Daten praktisch unbegrenzt gespeichert und nicht gelöscht werden.²¹³ Die Polizei entfernt Daten nicht, obwohl sie dazu gesetzlich verpflichtet ist, und es gibt nur wenige oder gar keine Durchsetzungsmechanismen oder Strafen, wenn dies geschieht.²¹⁴



Fazit

In diesem Bericht wird zusammengefasst, wie Polizei- und Strafjustizbehörden in Europa Vorhersagesysteme entwickeln, nutzen und betreiben, mit besonderem Fokus auf Belgien, Frankreich, Deutschland und Spanien. Dazu gehören Systeme zur Vorhersage von Kriminalität und zum Profiling sowie andere automatisierte datenbasierte Systeme und Datenanalysesysteme. Der Bericht analysiert außerdem Polizeidatenbanken und KI-basierte Videoüberwachungssysteme von Polizei und Gefängnisbehörden.

Der Bericht zeigt einen klaren Trend auf, dass Polizeikräfte zunehmend Systeme zur Vorhersage, zum Profiling und andere datenbasierte System zur Entscheidungsfindung einsetzen. Diese werden häufig von auf Überwachungstechnologien spezialisierten Unternehmen erworben, darunter auch Unternehmen, die wegen ihrer Verflechtung mit dem israelischen Staat in der Kritik stehen.

Der Einsatz von Systemen zur Vorhersage von Kriminalität gibt Anlass zu ernsthaften Bedenken hinsichtlich einer zunehmenden Kriminalisierung, Bestrafung – auch außerhalb des Strafrechtssystems – und Diskriminierung marginalisierter Personen und Gemeinschaften, insbesondere rassifizierter und wirtschaftlich benachteiligter Personen.

Der Bericht gibt zudem hinsichtlich der Genauigkeit dieser Systeme, des Mangels an Transparenz und wirksamer Rechenschaftspflicht sowie ihrer Rechtswidrigkeit Anlass zu erheblichen Bedenken. Daher unterstützen die Autor*innen dieses Berichts die Forderungen der Forschenden und Partnerorganisationen in Belgien, Frankreich, Deutschland und Spanien nach einem Verbot jeglicher Nutzung von KI und Algorithmen in der Strafverfolgung und im Strafrecht sowie nach strengen Transparenz- und Rechenschaftspflichten.

Diskriminierung

Standortbezogene Vorhersagesysteme enthalten keine Daten zu einzelnen Personen. Es sind jedoch vor allem rassifizierte Personen und Personen aus sozial schwachen Schichten, die in den Gebieten, in denen Kriminalität „vorhergesagt“ wird, Polizeikontrollen und möglichen Konsequenzen ausgesetzt sind.

Die Vorhersagen führen zu einer verstärkten polizeilichen Überwachung dieser Gebiete, der Menschen und Gemeinschaften in diesen Gebieten. Dies führt zu Racial Profiling, Kontrollen und Durchsuchungen von Personen in diesen Gebieten und in der Folge zu Kriminalisierung. Auf diese Weise liefern Instrumente zur Vorhersage von Kriminalität die Rechtfertigung für rassistische Konzentration auf bestimmte Gebiete und die dort lebenden Personen. Außerdem wird der vermeintliche rechtliche Schutz vor ethnischem Profiling umgangen.

Diese Kontrollen, Interventionen und Vorfälle im Rahmen der Strafverfolgung werden anschließend in Datenbanken erfasst, die wiederum in Vorhersagesysteme eingespeist werden. Die Verwendung der Daten für weitere Vorhersagen erzeugt eine Rückkopplungsschleife, in der dieselben Bereiche und Profile immer wieder ins Visier genommen werden.

Dasselbe Problem verzerrter Daten, die zu verzerrten Ergebnissen führen und Rückkopplungsschleifen fortbestehen lassen, tritt auch bei personenbezogenen Vorhersagesystemen auf. Das spanische System DRAVY weist zudem eine grundlegende Diskriminierung in seinem Design auf: Es konzentriert sich auf das westliche Konzept der sogenannten „dschihadistischen“ Radikalisierung und ist daher fast ausschließlich auf Muslime und Personen mit muslimischem Hintergrund ausgerichtet. Es weist zudem eine signifikante Falsch-Positiv-Quote auf. Ähnlich basiert das System RADAR-iTE in Deutschland auf Islamophobie und einer voreingenommenen Vorstellung davon, wer eine potenzielle „Bedrohung“ darstellt. Dies führt zu einer erheblichen antimuslimischen Voreingenommenheit in seinen Ergebnissen und bei den Betroffenen.



Kriminalisierung

Systeme für die Vorhersage von ortsbezogener Kriminalität stufen ganze Stadtteile als kriminell ein und prognostizieren, dass dort hohe Kriminalitätsraten auftreten. Dies führt zu verstärkter Polizeipräsenz und gezielten Kontrollen durch Streifen, zu Personenkontrollen und anderen Maßnahmen. Darüber hinaus werden praktisch „verdachtslose“ Kontrollen, Identitätsprüfungen und Durchsuchungen gerechtfertigt – die Vorhersage liefert sowohl die Rechtfertigung als auch den Verdacht. Dies erhöht die Wahrscheinlichkeit der Kriminalisierung der Personen und Gemeinschaften, die in diesen Gebieten leben und arbeiten. Dies kann ohne objektive Beweise für ein strafbares Fehlverhalten geschehen.

Personenbezogene Systeme erstellen Profile von Personen anhand ihres Hintergrunds und stempeln sie entweder direkt als kriminell ab oder stigmatisieren sie indirekt als potenziell kriminell. Diese Personen werden dann als schuldig betrachtet und behandelt, bis ihre Unschuld bewiesen ist. Personen wurden durch Profiling-Systeme auch mit anderen Personen in Verbindung gebracht, die selbst als kriminell eingestuft sind. Dies führt zu einem unglaublich weiten Netz der Kriminalisierung.

Individuelle „Vorhersagen“ oder Profile können schwerwiegende strafrechtliche und nichtstrafrechtliche Konsequenzen und Strafen nach sich ziehen. Wie in diesem Bericht zusammenfasst wird, gehören Überwachung und Beobachtung durch Polizei oder Strafverfolgungsbehörden, Hausbesuche oder Besuche am Arbeitsplatz, Razzien, Arbeitsverbote, Befragungen oder sogar Festnahmen und „präventive“ Inhaftierung zu den bekannten Folgen. Personen wurden aufenthaltsrechtlichen Untersuchungen unterzogen. Sie wurden Grenzkontrollen und Befragungen unterzogen, die zur Einreiseverweigerung führten, ihre Asylanträge wurden ausgesetzt oder gestoppt und sie wurden sogar abgeschoben. All dies kann ohne objektive Beweise für ein strafbares Fehlverhalten geschehen: nur aufgrund datenbasierter, algorithmisch generierter Verdächtigungen.



Transparenz und Rechenschaftspflicht

Der Mangel an Transparenz bei der Entwicklung, Schulung und operativen Nutzung dieser Systeme zur Vorhersage, zum Profiling und zur Risikobewertung stellt ein grundlegendes Hindernis für Gerechtigkeit und Rechenschaftspflicht dar.

Personen, die aufgrund von Systemen zum Predictive-Policing oder zur Vorhersage von Kriminalität ins Visier der Polizei oder der Strafverfolgungsbehörden geraten, sind sich dessen oft nicht bewusst. Die Behörden, die diese Systeme nutzen, geben in der Regel keine Informationen über diese Systeme oder deren Einsatz preis. Sie informieren die Betroffenen auch nicht darüber, dass sie Gegenstand von Profiling, Prognosen oder Risikobewertungen waren oder dass die gegen sie ergriffenen Maßnahmen von solchen beeinflusst wurden. Dies wirft Fragen zur Fairness und Unparteilichkeit der Systeme und der von ihnen beeinflussten Prozesse auf.

Europaweit schreiben die rechtlichen Rahmen keine ausreichende Transparenz dieser Systeme vor. Die geplante KI-Verordnung der EU sieht in diesem Zusammenhang keine sinnvollen Transparenzanforderungen vor. Es enthält weitreichende Ausnahmen für Systeme zur Aufdeckung, Verhütung, Untersuchung und Verfolgung von Straftaten.

Das muss sich ändern. Polizei und Strafverfolgungsbehörden müssen die Details aller von ihnen verwendeten datenbasierten, algorithmischen oder automatisierten Systeme in einer öffentlich zugänglichen Datenbank oder auf einer Website veröffentlichen. Dies umfasst Angaben zum System oder der Software und der Funktionsweise, die verwendeten Daten, die Art und Weise, wie das System Analysen durchführt oder Ergebnisse erstellt, und wofür diese verwendet werden, sowie die möglichen Folgen.

Sollten Einzelpersonen oder Gruppen aufgrund eines automatisierten Entscheidungsfindungssystems oder datenbasierter Analysen polizeiliche oder strafrechtliche Konsequenzen erleiden, müssen sie darüber informiert werden. Die Polizei oder die Strafverfolgungsbehörde muss die betroffene Person benachrichtigen und ihr Informationen darüber geben, wie sie diese Entscheidung oder dieses Ergebnis anfechten kann. Diese Informationen müssen in einem



Format und auf eine Weise bereitgestellt werden, die auch für Personen ohne Fachkenntnisse oder Kenntnisse dieser Systeme verständlich ist.

Einzelpersonen und Gruppen müssen klare Möglichkeiten haben, die Ergebnisse oder Folgen eines solchen automatisierten Entscheidungsfindungssystems anzufechten und gegebenenfalls wirksame Rechtsmittel einzulegen.

Keine Rechtsgrundlage und rechtswidrige Nutzung

Viele dieser umstrittenen Systeme werden ohne ausreichende Rechtsgrundlage für ihre Nutzung entwickelt, getestet oder betrieben. In vielen Fällen werden sie ohne Rechtsgrundlage betrieben und in einigen Fällen, wie in Deutschland, wurden sie für rechtswidrig befunden. Wie in Frankreich wurde die diesen Systemen zugrunde liegende Datenerhebung ebenfalls für rechtswidrig befunden.

Ungenauigkeit

In vielen Fällen sind diese Systeme grundsätzlich ungenau. Sie produzieren schwerwiegende Ungenauigkeiten oder Fehllarme, die möglicherweise Unschuldige belasten. In vielen Fällen haben Polizei, Strafverfolgungsbehörden oder Strafjustizbehörden ihre Genauigkeit vor dem Einsatz nicht ausreichend oder angemessen bewertet. Selbst nach Abschluss solcher Tests wurden Systeme mit unzureichender Genauigkeit teilweise weiterhin verwendet.

Genauigkeit ist jedoch kein Allheilmittel. Ein „genaues“ System würde lediglich dazu dienen, die den verwendeten Daten innewohnende Diskriminierung aufrechtzuerhalten und zu reproduzieren.

Verbot

Wie dieser Bericht zeigt, führen die standort- und personenbezogenen Systeme zur Vorhersage, zum Profiling und zur Risikobewertung zu rassistischem und sozioökonomischem Profiling, Diskriminierung und Kriminalisierung.

Ihr Einsatz führt zu ungerechten und diskriminierenden Konsequenzen – von Überwachung bis hin zu Personenkontrollen, von polizeilichen Schikanen und Gewalt bis hin zu Festnahmen, von Inhaftierung bis hin zur Abschiebung.



Das Fazit dieses Berichts und derjenigen, die ihm zugrunde liegen, ist dasselbe: Diese Systeme müssen verboten werden.

Wo diese Systeme eingesetzt werden, sollten die nationalen Gesetzgeber ihre Nutzung gesetzlich verbieten. Ebenso sollten, wo diese Systeme eingesetzt werden, lokale Gesetzgeber oder Räte, wie z. B. Stadt- oder Gemeinderäte, versuchen, in ihrem Zuständigkeitsbereich ein Verbot zu erlassen.²¹⁵

Es gibt in Europa und anderswo aktuelle und langjährige Kampagnen gegen den Einsatz dieser Systeme, wie beispielsweise die Kampagne zum Verbot von Systemen zum Predictive Policing in der KI-Verordnung der EU,²¹⁶ die *Technopolice*-Kampagnen in Frankreich²¹⁷ und Belgien,²¹⁸ die Koalition „*Safety Not Surveillance*“ im Vereinigten Königreich²¹⁹ und „*Stop LAPD Spying*“ in den USA.²²⁰ Die Unterstützung dieser und ähnlicher Kampagnen ist unerlässlich, da Regierungen, Polizeikräfte, Strafverfolgungsbehörden und Unternehmen den Einsatz algorithmischer, automatisierter und KI-basierter Systeme ausweiten wollen.



“

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.



Bildnachweise

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

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

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

Page 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

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

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

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

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

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

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

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

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

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

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

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

Page 34: [“manifest contre la «Loi Sécurité globale» à Paris le 28 novembre 2020 \(2\)”](#) by Jeanne Menjoulet

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Endnoten

- 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 Europcop, 'Analysis and prediction of crime', <https://www.>

- 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/>

expedientappendixblobobservlet?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/10.1002/9781119184256.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>

- 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-gefahrder-101.htm>
- 165 Deutscher Bundestag, 'Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökyay 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://stoplapdspeying.org/>