NEW TECHNOLOGY, OLD INJUSTICE.

DATA-DRIVEN DISCRIMINATION AND CRIMINALISATION IN POLICE AND PRISONS IN EUROPE

JUNE 2025

STATEWATCH

WRITTEN BY:
Griff Ferris
Sofia Lyall

SUPPORTED BY:
European Artificial Intelligence & Society Fund

Publication information

About this report

Authors: Griff Ferris, Sofia Lyall

Editor: Chris Jones

Design: McKensie Marie

This report was supported by the European AI & Society Foundation.

Published by Statewatch, May 2025

Support our work

Support our work to expose state power and inform dissent by making a donation. And join our mailing list to stay informed and help spread ourwork.

Scan the QR code above or visit:

— Donation page

— Mailing list sign-up

About Statewatch

Statewatch produces and promotes critical research, policy analysis and investigative journalism to inform debates, movements and campaigns for civil liberties, human rights and democratic standards.

statewatch.org
(+44) (0) 203 393 8366
MayDay Rooms, 88 Fleet Street,
London EC4Y 1DH,UK

Registered UK charity number:
1154784

Registered UK company number:
08480724

Registered company name: The Libertarian Research & Education Trust

Registered office: 88 Fleet Street, London EC4Y 1DH, UK.

Contents

Acknowledgements

This work has been made possible by researchers and partner organisations in Belgium, France, Germany and Spain:

— Belgium: Corentin Debailleul, Technopolice Belgium and La Ligue des droits humains;

— France: Edlira Nano and Félix Tréguer, La Quadrature du Net, with assistance from members of the Technopolice France working group of La Quadrature du Net;

— Germany: Sonja Peteranderl, AlgorithmWatch;

— Spain: Naiara Bellio, with collaborators Ana Valdivia and Javier Sánchez Monedero, AlgoRace.

We are grateful to all of the people and groups who participated in interviews or otherwise provided information, experience or expertise.

We also want to thank the work of people and organisations who challenge and organise against racism and discrimination in policing and criminal legal systems, of which these new technologies are just the latest iteration.

Definitions

Artificial intelligence

> *"...a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments"*[1]
>
> - European Union Artificial Intelligence Act's definition of an AI system

This report uses this definition, though there are many ways to define AI and AI systems.[2] It is important to note that most of the data-based, algorithmic and automated systems used by police and criminal justice authorities in Europe do not use artificial intelligence. Some of these systems use machine learning (see below), a sub-field of AI. However, the majority of these systems use classic statistical methods and can be described as automated-decision making systems (see below).

Automated decision-making system

The United Kingdom Office for AI defines automated decision-making systems as those which employ "solely automated decisions (no human judgement involved)," as well as "automated assisted decision-making (assisting human judgement)."[3]

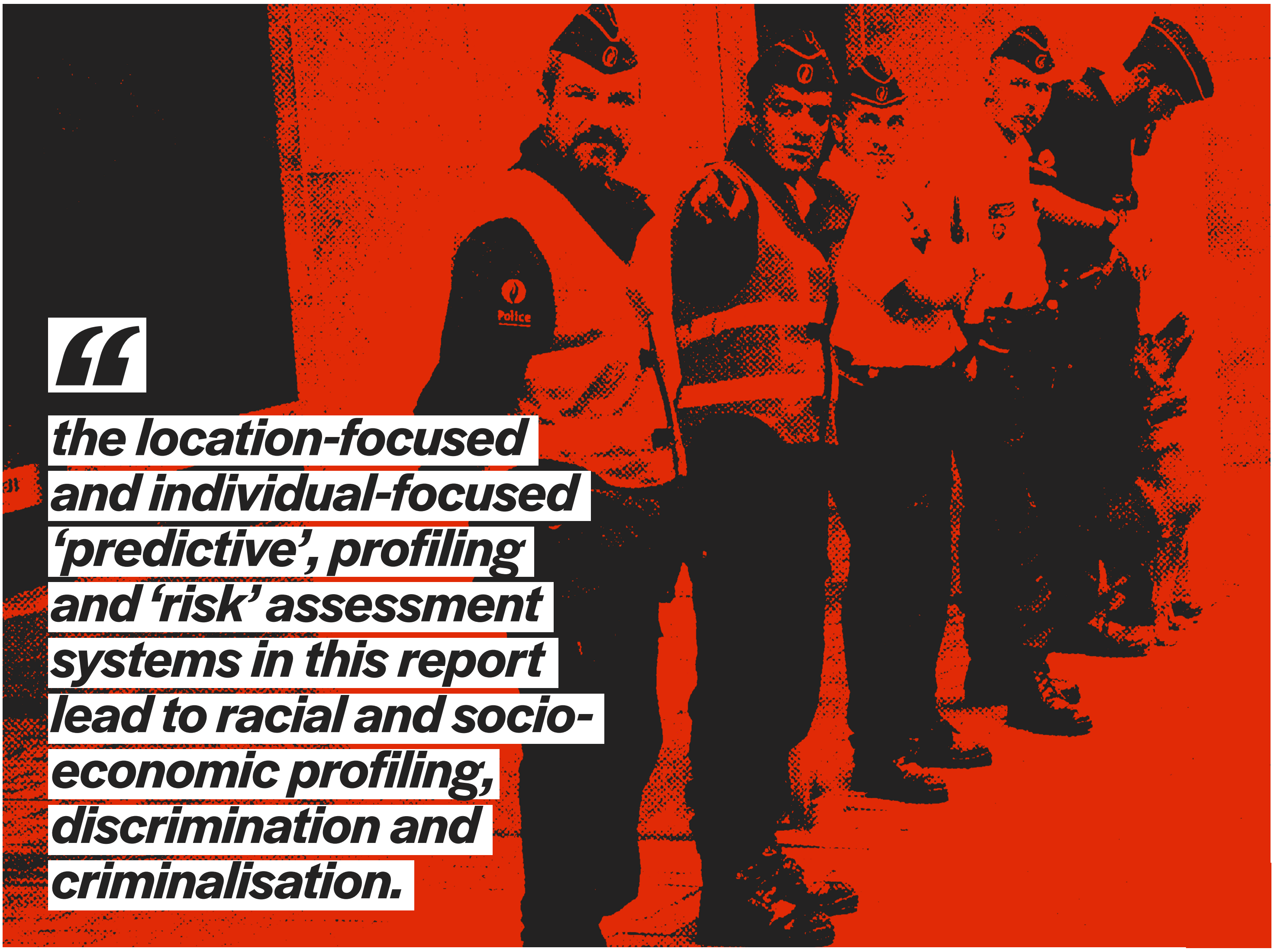
Machine learning

The Cambridge Dictionary defines machine-learning as "the process of computers improving their own ability to carry out tasks by analysing new data, without a human needing to give instructions in the form of a program, or the study of creating and using computer systems that can do this".[4]

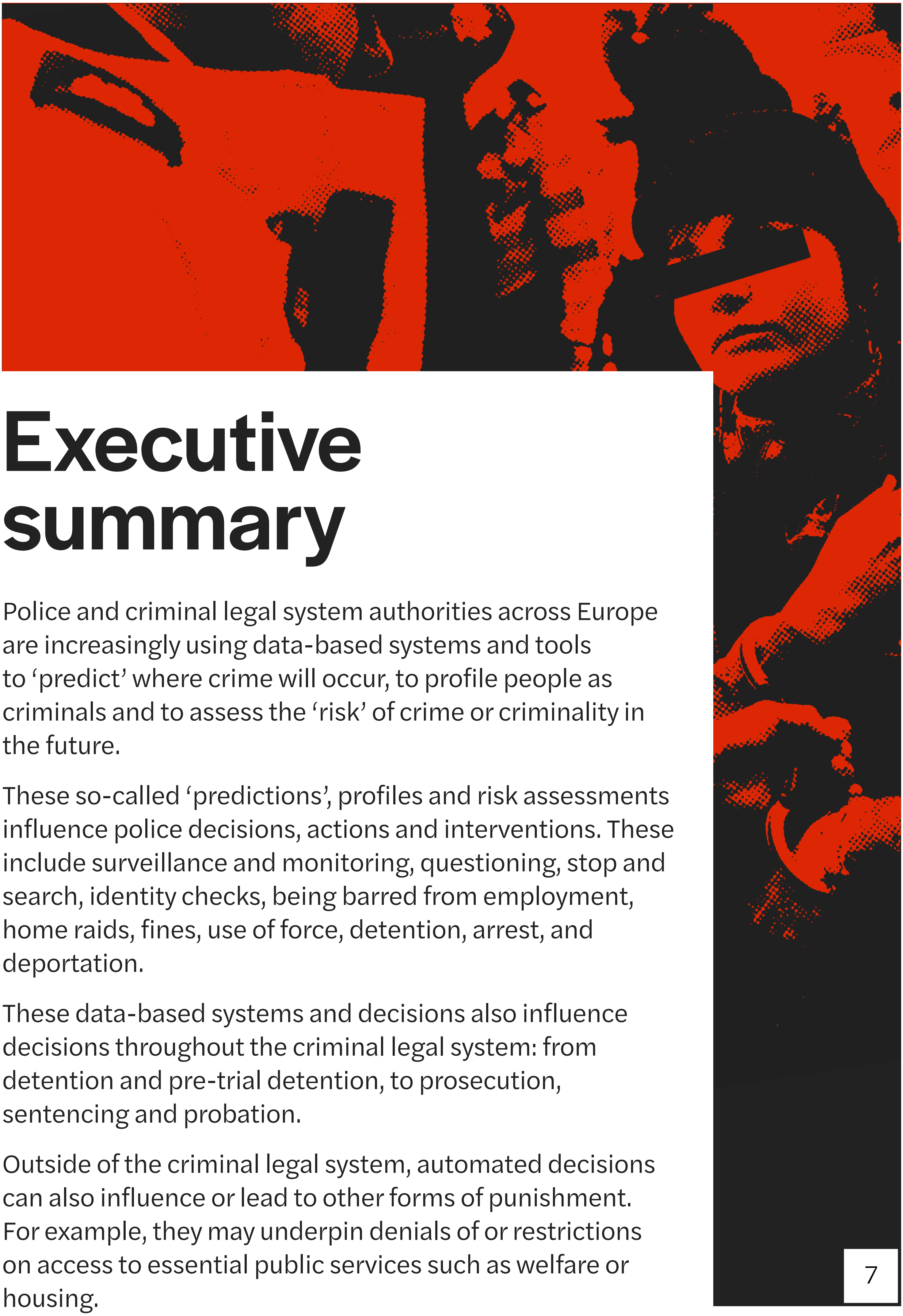
‘Predictive’ policing:

There are two main types of so-called predictive policing: location or place-based, and person-based. This report uses the definition by Amnesty International.

> *“…computer programs that use data and algorithmic models to assess the risk that a crime will be committed. Predictive policing systems calculate risk scores that allegedly reflect the likelihood that a person or group is or will be a victim or perpetrator (person- based predictive policing), or that a specific location will be a future crime scene (place-based predictive policing). Based on these computer-generated risk scores, the police take measures seeking to prevent or detect the predicted crime by directing policing efforts towards ‘high-risk’ locations, individuals, or groups.”*[5]
>
> - Amnesty International’s definition of predictive policing



“*the location-focused and individual-focused ‘predictive’, profiling and ‘risk’ assessment systems in this report lead to racial and socio-economic profiling, discrimination and criminalisation.*”



Executive summary

Police and criminal legal system authorities across Europe are increasingly using data-based systems and tools to ‘predict’ where crime will occur, to profile people as criminals and to assess the ‘risk’ of crime or criminality in the future.

These so-called ‘predictions’, profiles and risk assessments influence police decisions, actions and interventions. These include surveillance and monitoring, questioning, stop and search, identity checks, being barred from employment, home raids, fines, use of force, detention, arrest, and deportation.

These data-based systems and decisions also influence decisions throughout the criminal legal system: from detention and pre-trial detention, to prosecution, sentencing and probation.

Outside of the criminal legal system, automated decisions can also influence or lead to other forms of punishment. For example, they may underpin denials of or restrictions on access to essential public services such as welfare or housing.

This report synthesises **original research about automated decision-making systems and databases used in the policing and criminal legal systems** in four countries: Belgium, France, Germany and Spain. It is based on in-depth research conducted by partner organisations in those countries. It looks at:

- how these data-based crime prediction systems are developed;
- how they are used by law enforcement and criminal legal system authorities;
- the outputs produced by the systems;
- how these outputs are used and influence decisions, and the impact these have on people, groups and communities.

It also considers how marginalised groups and communities are disproportionately targeted and impacted by these systems, including Black and racialised people and communities, victims of gender-based violence, migrants and people from working-class and socio-economically deprived backgrounds and areas, and people with mental health issues.

The majority of these systems use historical data, for example from the police or criminal legal system. This reflects historic and existing biases within these institutions and within wider society. This leads to the over-policing and criminalisation of marginalised communities, particularly racialised groups, migrants, and people from low-income neighbourhoods.

The use of these systems in policing and the criminal legal system has significant consequences for individuals' rights, including the right to a fair trial, privacy, and freedom from discrimination.

Location-focused 'predictive' policing systems

Across Europe, police forces are developing and implementing location-focused methods of 'predictive' policing. These algorithmic systems are developed to 'predict' where and when a crime will occur. This allows police to allocate resources to these locations. Geographic crime 'prediction' systems are used or have been used in all four countries examined: Belgium, France, Germany and Spain, as well as in other European countries, for example: Italy, the Netherlands, Switzerland and the UK.

The research identified two main types of location-focused systems:

- crime 'hotspot' prediction, which draws on historical policing data to forecast future crime locations; and
- environmental 'risk' prediction algorithms, which are based on the assumption that environmental factors determine where crimes take place, and can therefore predict 'risky' locations.

Crime 'hotspot' prediction methods use historical crime statistics on where and when a crime took place to 'predict' future crime locations or 'hotspots'. These predictions are based on the analysis of statistical insights and trends from large amounts of crime data, often from police databases. Generally, 'hotspot' prediction systems provide police with a 'heat map' to identify areas or locations where there is allegedly a high risk of crime taking place.

Crime 'hotspot' prediction systems are used to allocate police resources and determine where and when officers should patrol. Outcomes in 'hotspot' areas may include: surveillance, information-gathering, identity checks, questioning, searches, restraining orders, home raids, and arrests. **The research raises concerns that locations labelled as crime 'hotspots' are disproportionately areas**

or neighbourhoods where low-income and racialised communities live and work.

Location-focused systems are based on environmental and contextual data. They draw on environmental or contextual data to identify areas or locations that are allegedly more prone to criminality. An algorithm assigns a vulnerability value to locations based on spatial factors, including:

— whether the location is well-lit;

— metro or bus stations;

— outdoor seating areas of cafés;

— fast-food outlets;

— public toilets;

— pharmacies, bars, certain types of shops;

— trees and benches; and

— schools and post offices.

This method raises similar issues of bias and discrimination to those arising from systems based on crime data.

Person-focused 'predictive' policing and crime 'prediction' systems

Person-focused crime 'prediction' tools are designed to predict a person's likelihood or 'risk' of committing a criminal offence. Similar systems are used to assess people's likelihood of being a victim of crime, such as gender-based violence, or to detect allegedly false crime reports.

People targeted by these systems are subjected to a constant analysis of data that characterises them, their past and present lives and their relationships. The objective is to determine and 'predict' their behaviour, 'risk', or supposed 'criminality'. This can have serious

consequences. **The outputs generated by these systems may lead to people being put under surveillance or monitoring. They may result in increased police stops, questioning, searches, home or workplace visits, being barred from employment, detention, deportation, or arrest.**

These tools are also used in the criminal legal system, and can influence judges' decision-making, including sentencing. They can influence the length of a person's imprisonment and when they will be released, as well as the conditions in which they are detained.

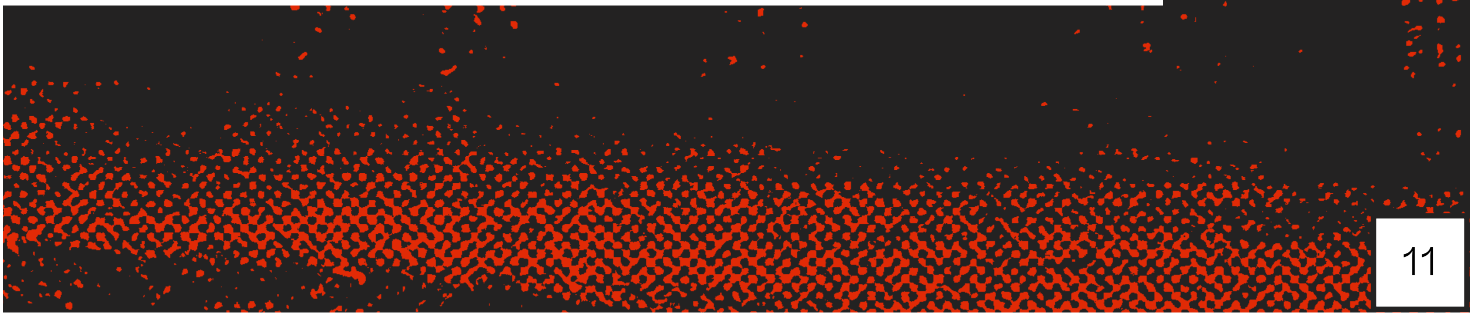
Conclusion

The use of these systems leads to racial and socio-economic profiling, discrimination and criminalisation. This is directed particularly against marginalised people and communities, specifically Black and minoritised ethnic people, and people from deprived backgrounds.

Their use leads to unjust and discriminatory consequences: from surveillance, identity checks and searches, to police harassment, home raids, being barred from employment, arrest, detention and deportation.

These systems are used secretively, meaning that people are not aware of their use. As a result, people targeted by them and the actions that results from their outputs are unable to challenge them. Even if they were, there is no clear framework for accountability.

The conclusion of all of the partner reports, and of this report, is the same: that these systems must be prohibited.



Introduction

Across Europe, police and criminal justice authorities are using an increasing array of digital and data-based systems. New systems are being introduced at a dizzying rate, with little transparency around their deployment, or prior consideration of their effects and consequences.

These systems include:

— facial recognition surveillance;

— emotion recognition systems;

— mobile phone extraction tools;

— electronic tagging and ankle monitors; and

— ‘predictive’ and profiling systems.

What these practices all have in common is the gathering and processing of massive quantities of data – often sensitive personal data – to inform decision-making.

This report focuses on data-based, algorithmic and automated decision-making systems used by police forces to ‘predict’ where or when crimes will be committed, or by whom. Proponents of these supposedly scientific and ‘predictive’ approaches argue that they allow police forces to improve the efficiency of their operations, while also reducing costs:

> *“By using a new strategy called “Evidence-Based-Policing,” governments can work transparently with police and the public to invest in police tasks that are cost-effective. These investments can be made while cutting police budgets by putting an end to expensive but ineffective police tasks.”*[6]

Indeed, the AI coordinator for France’s ***Gendarmerie Nationale***, Colonel Patrick Perrot, has claimed that data-based methods allow police to anticipate crimes before they occur:

> *“…the scientific approach enables us to develop modelling techniques capable of understanding and preparing for future developments. The notion of anticipation is now a determining factor in the field of crime.”*[7]

This has, in turn, led to increased scrutiny of so-called ‘predictive’ policing systems from civil society organisations, political activists and organisers, and academics across Europe.

Many groups have raised serious concerns about the potential consequences of these systems – for example, surveillance, monitoring, questioning, stop and search, fines, home raids, use of force, deportation, detention, and arrest – as well as the potential infringements on individual rights. These systems engage and potentially infringe the right to a fair trial, privacy, freedom from discrimination, the presumption of innocence and the right to an effective remedy.[8]

The research brought together in this report adds to these concerns. It seeks to support campaigns taking place internationally, nationally, regionally and locally to call for prohibitions on the use of AI and algorithms by criminal justice authorities. Where bans have not yet been introduced, procedural safeguards are needed, including rigorous pre-deployment testing, public transparency requirements, and meaningful opportunities for redress.

Report outline

This report brings together and summarises in-depth research about 'predictive' systems and databases in policing and criminal legal systems in Europe, based on research in four countries: Belgium, France and Germany and Spain.

These countries were primarily chosen for two reasons. It was known that 'predictive' systems were being widely-used by police forces and in the criminal legal system. However, there was little publicly-available research on the systems' development, use and impact.

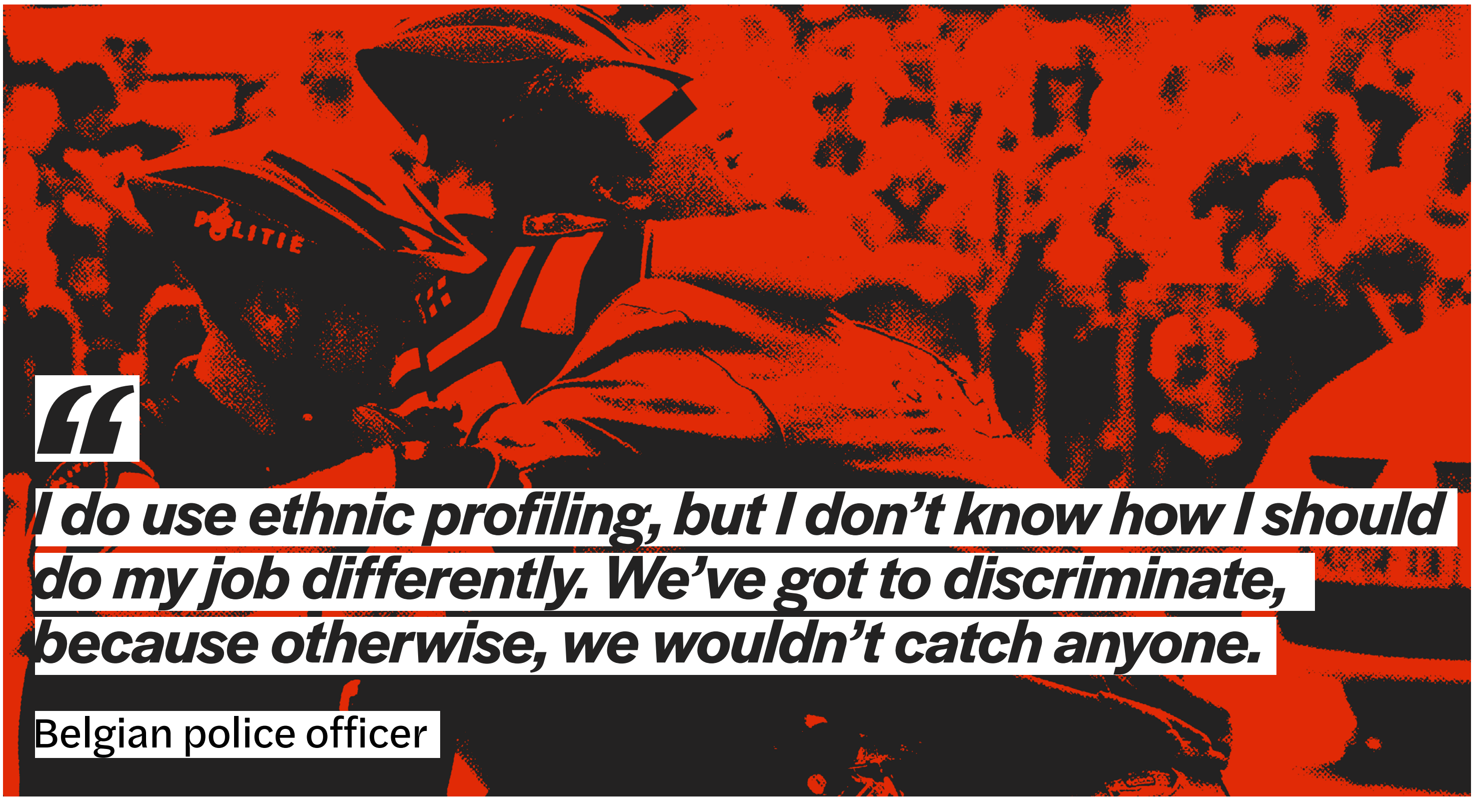
This research was conducted over the course of 2023 and 2024 by researchers with ***AlgoRace***, ***AlgorithmWatch***, ***La Quadrature du Net***, ***and Technopolice***. **The original versions are available online.**

In each country, researchers worked to expose the 'predictive' systems in use, how they work, the outputs they produce, and the impacts these have on people, groups, and communities.

That research is combined in this report to provide an overview of the landscape, trends, and consequences of 'predictive' policing in Belgium, France, Germany and Spain. It also includes other research and reports on the use of predictive and profiling systems in policing and criminal legal systems elsewhere in Europe, including the Netherlands, Italy, the Netherlands, Switzerland and the UK.

Four sections of the report examine the data-driven 'predictive' systems used by police forces: location-focused systems, person-focused systems, AI video surveillance, and databases. Drawing together some of the key examples from each country, each section covers the purposes, data inputs, and outcomes of the systems.

The final section of the report analyses the key concerns and infringements on individual rights, including discrimination, criminalisation, transparency, accountability, and unlawfulness.



> **“I do use ethnic profiling, but I don’t know how I should do my job differently. We’ve got to discriminate, because otherwise, we wouldn’t catch anyone.**
>
> Belgian police officer

Structural and institutional discrimination

The majority of crime ‘prediction’ systems use historical crime data. This reflects the existing institutional racism, discrimination and biases within police and criminal justice institutions and wider society.

The discriminatory police practices of racial and ethnic profiling have long been criticised by victims, victims’ associations, academics, human rights organisations and international organisations. It results in stops, identity checks and searches based on racialised characteristics such as skin colour or (presumed) religious affiliation.

A 2017 study by the EU Fundamental Rights Agency that surveyed people in each of the then-28 EU member states found that almost half of survey respondents from certain minoritised ethnic communities were stopped by police. This included people “with Sub-Saharan African backgrounds” in Luxembourg and Finland, people with “North African backgrounds” in the Netherlands, and Roma in Greece and Portugal.[9]

The majority of people ‘of African descent’ stopped by police across the EU perceived it to be racially motivated, according to the EU’s own Agency for Fundamental Rights (FRA).[10] In France, young men perceived to be Black or Arab are 20 times (2000%) more likely to be stopped by police than the rest of the population, according to the country’s human rights ombudsman.[11]

In Belgium, there is a lack of official information on ethnic profiling, as there has historically been no requirement for police to make a record of the stops and checks they make. However, Amnesty International interviewed Belgian police officers who themselves admitted racial profiling existed in policing. One was quoted as saying "I do use ethnic profiling, but I don't know how I should do my job differently. We've got to discriminate, because otherwise, we wouldn't catch anyone."[12]

Police in Spain disproportionately stop and search people based on their racial, ethnic, or religious appearance. This has been well-documented by multiple studies.[13] People from North Africa, Sub-Saharan Africa and Eastern European countries are more likely to be subjected to identity checks than Spanish people.[14]

In Germany, individuals with foreign citizenship are overrepresented among the suspects recorded by the police, those convicted by the courts, and those imprisoned.[15] In Belgium, a study found that people on trial who had a name perceived as Muslim were more likely to be convicted than people with a name perceived as while Belgian, all other things being equal.[16] In France, non-nationals are three times more likely to be held in pre-trial detention,[17] while 45% of people held in pre-trial detention in Belgium are not Belgian nationals.[18]

Despite this clear evidence, discrimination by police, law enforcement and the criminal legal system is still not widely recognised or acknowledged as a structural or institutional problem in many European countries. As the Black authors of the Afrozensus 2020, a survey of 6000 Black, African and Afro-diasporic people in Germany, point out:

> ***"…the general public is still preoccupied with the question of whether there really is institutional racism within the German police force or whether these are supposedly isolated cases. This is not a question for Black, African and Afro-diasporic people, for whom it is a reality of life."***[19]

This data, which represents institutional and systemic discrimination, is used in 'predictive', profiling and 'risk' assessment systems by law enforcement and criminal legal system authorities.

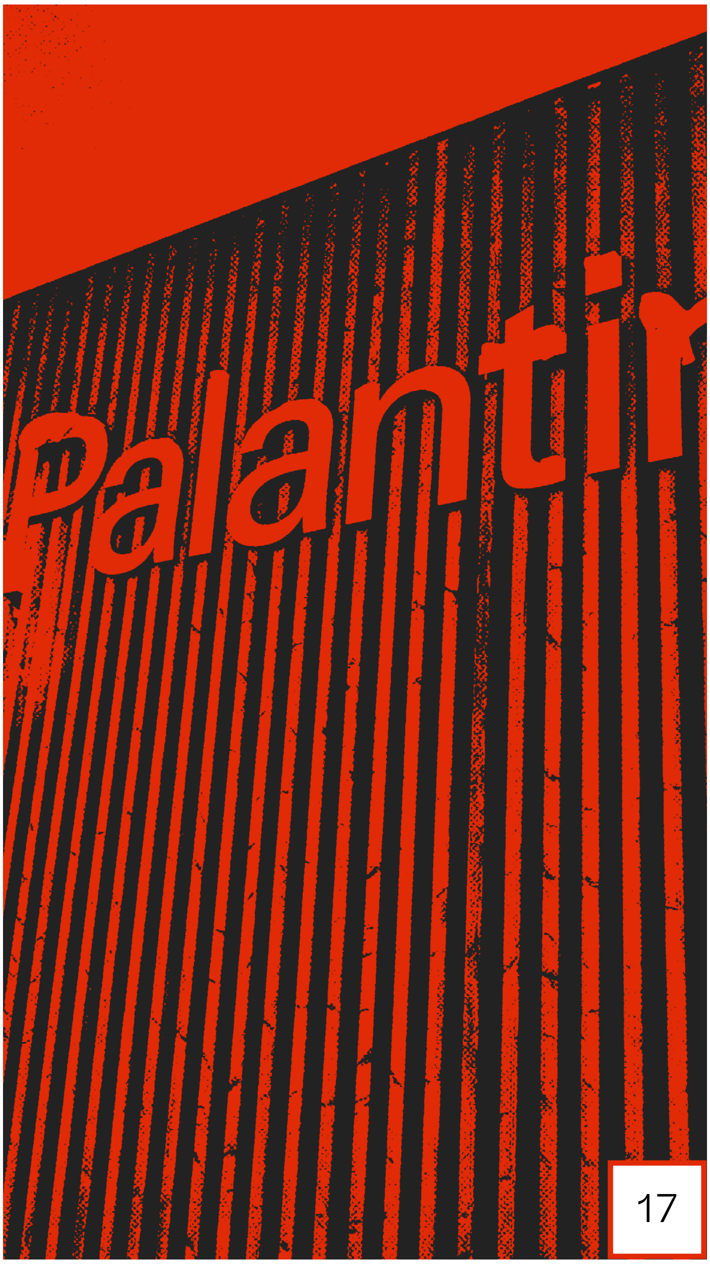
Corporate involvement

Private companies are significant actors in the digitisation and automation of policing. Many of the systems identified by researchers in Belgium, France and Germany are supplied to police forces by private security companies, usually through competitive tender processes. Other data-driven systems are developed 'in-house', or in collaboration with academic researchers.

The largest and most notorious tech corporation selling 'predictive' policing software in Europe is the American company, Palantir. Three of Germany's 16 federal states currently use the company's systems.[20] Palantir's global revenue in 2024 was $2.87 billion.[21] It is internationally known for its ties to secret services, militaries and other government bodies.[22]

Other key companies providing data-driven systems to police forces in Europe include:

- Briefcam, an Israeli company producing AI video surveillance;[23]
- ClearView, an American facial recognition company, primarily providing software to law enforcement authorities;[24]
- **Edicia**, a French company developing 'urban security' software;
- Simsi, who partnered with the US-based Rutgers University in New Jersey as the commercial provider of the **Risk Terrain Modelling system**;
- **EuroCop** in Spain, who have signed more than 100 contracts with public administrations in the last two decades;[25]
- **Securitas**, a Swedish company offering "security solutions"; and



- SopraSteria, a French company that also holds contracts with the EU to develop one of its vast biometric policing and immigration systems.[26]

Alongside Briefcam, other Israeli companies hold contracts with Belgian authorities, namely TA9/ Rayzone and Interionet. **The origins of TA9 are particularly concerning: the CEO formerly served as deputy director of Unit 8200, the intelligence unit of the Israeli military supposedly responsible for developing the army's AI systems.**[27] Unit 8200 has played host to multiple officials who went on to found private security companies.[28]

The surveillance tech industry is currently booming.[29] One estimate puts the annual global growth rate at 12.5%, meaning an industry worth $186 billion in 2025.[30] Given how lucrative the industry clearly is, we can only expect that the number of 'predictive' systems, and the companies that supply them, will grow in the coming years.

> ***“Given how lucrative the industry clearly is, we can only expect that the number of 'predictive' systems, and the companies that supply them, will grow in the coming years.***

The European Union Artificial Intelligence Act (EU AI Act)

The EU AI Act is a global landmark legal framework for regulating AI, based on its potential risks to health, safety and fundamental rights. It was approved in June 2024 after lengthy and complex negotiations in the European Parliament. The first elements of the Act came into force in February 2025.

The AI Act sets out a number of "prohibited AI practices." These include:

- 'predictive policing';
- remote biometric identification (such as public facial recognition);
- "social scoring"; and
- emotion recognition.[31]

The Act's prohibition on crime 'prediction' systems is vague and unclear, and contains a huge exemption that will significantly limit its impact. It is possible that many if not all of the systems covered in this report and the underlying research will not be prohibited by the Act. With regard to predictive policing systems, it prohibits:

> ***"...the placing on the market, the putting into service for this specific purpose, or the use of an AI system for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics".***

However, it then goes on to say:

> ***"...this prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity."***[32]

The law appears to prohibit ***some*** AI systems that make predictions about individuals based on "profiling... personality traits or characteristics". However, it does not apply to AI systems which "support" human assessment. This late addition to the text effectively renders the ban meaningless. Law enforcement authorities can simply state, as they already do, that their use of AI systems is to "support" human assessment.

Further, the text does not clearly refer to or prohibit location-focused or geographic crime prediction systems which are used widely across Europe. The European Commission's guidelines on prohibited AI practices makes clear that they do not fall within the scope of the prohibition.[33] The guidelines are, however, non-binding. Should there be legal challenges to systems of this type, the Court of Justice of the European Union (CJEU) may have the final say.

The prohibition has been described as only a “partial” ban, and is substantially weaker than an original version voted for by the European Parliament in June 2023.[34] EU governments and big tech worked hard to water down safeguards in the Act.[35]

The AI Act does contain some very basic transparency measures. It stipulates that in certain cases, where systems are classed as ‘high-risk’, people should be informed about the fact that an AI system is in use.[36] If an individual is subject to a decision based on an output from a high-risk AI system that produces legal effects, or that significantly affects that person in a way they consider to have an adverse impact on their health, safety or fundamental rights, they has the right to a “clear and meaningful explanation” of the role of the AI system in that decision.[37]

However, there is a significant exemption for systems which are used to detect, prevent, investigate and prosecute criminal offences.[38] **As a result, there are effectively no transparency measures for ‘predictive’ policing and crime ‘prediction’ systems in the Act.**

In addition, there is no meaningful mechanism by which those affected by a ‘prohibited AI practice’ or AI systems that do not comply with the Act can challenge such systems, or seek redress for the harms that arise from the use of AI systems.[39] Individuals affected can complain to a national authority, but there is no obligation in the Act for those authorities to offer any remedy.[40]

There are standards in existing data protection legislation, namely the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED), the latter of which applies to law enforcement use of data and automated decision-making systems. The Law Enforcement Directive prohibits decisions based ***solely*** on automated processing. However, as above, this may render the prohibition meaningless. Law enforcement authorities can simply claim that the decisions were not based solely on automated processing.

Methodology

The research on Belgium, France, Germany and Spain that forms the basis of this report was conducted by researchers and investigators in those countries, using a range of methods, supported by the editors of this report:

— ***Interviews:*** The researchers conducted interviews with experts, academics and other researchers, as well as developers of the data-based and automated decision-making systems. They also interviewed police officials and other officials responsible for operating these systems. Most importantly, they interviewed and spoke to people and groups impacted by these systems and the police and criminal legal system action they influenced, and people working with these groups.

— ***Freedom of information requests:*** Researchers sent used freedom of information laws to send requests to local and national police forces, government departments and prison and probation authorities.

— ***Open-source research:*** Researchers searched public documents such as contracts, financial records, internal evaluation reports and studies, impact assessments, company websites and brochures, and related information.

— ***Review of existing academic literature:*** Researchers reviewed and analysed studies and reports on these systems, especially technical studies on their design, training and operation.

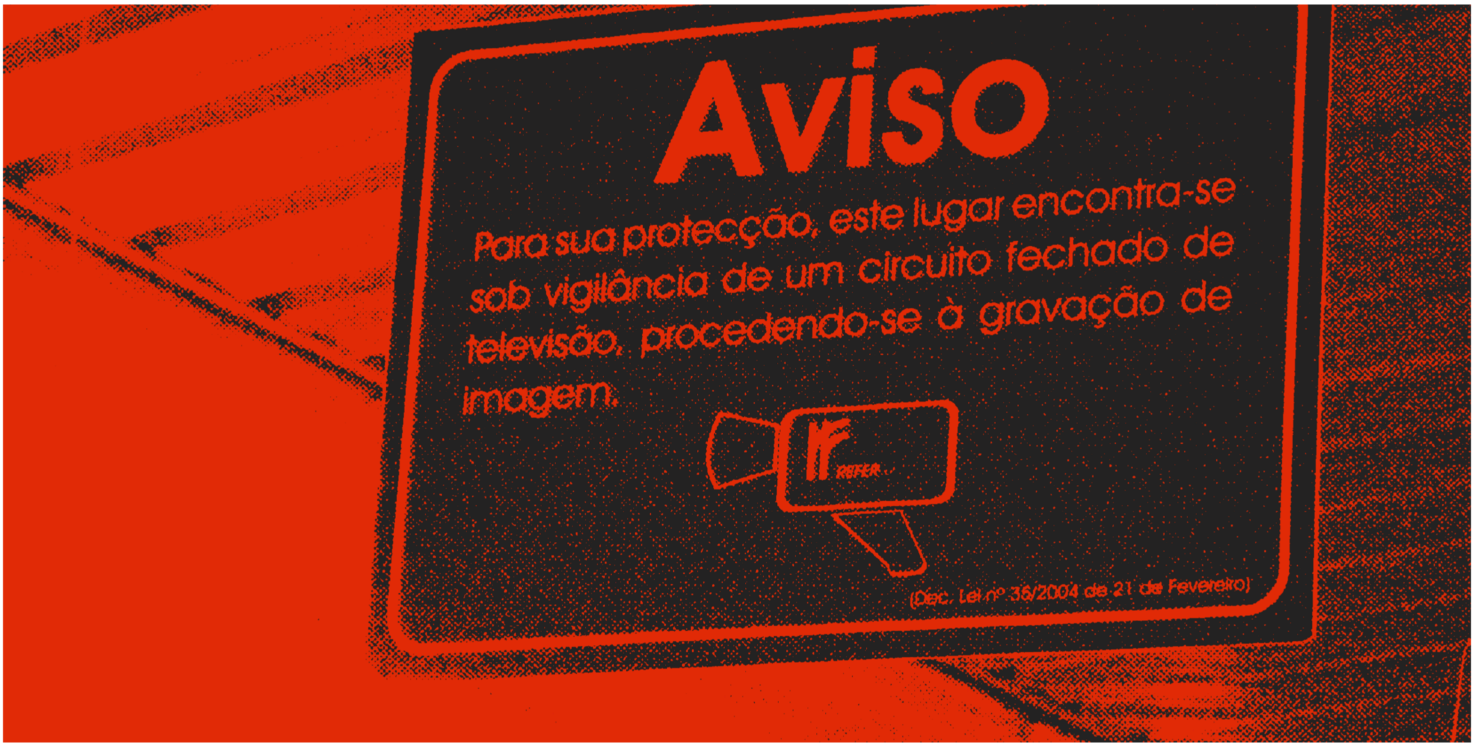
Transparency issues

It is clear from all the country research that police and criminal justice authorities seek to restrict and prevent the release or publication of information about 'predictive', profiling and risk assessment systems.

In all countries, researchers' formal requests to government departments, police forces, and local authorities were rejected or ignored – often on the basis of commercial secrecy, or threats to national security.[41] Where government departments did respond, information was often sparse and evasive.[42] Private companies, meanwhile, provide significant infrastructure and operational tools for the police. However, they are not covered by freedom of information laws.[43]

Similarly, requests for interviews were often rejected or ignored. In Spain, ***AlgoRace*** made multiple requests for interviews to government departments. They were rejected, despite the subjects of the requests agreeing to speak individually.

The level of transparency surrounding these systems is completely unacceptable, especially considering the serious technical, legal and political issues they raise.


Aviso
Para sua protecção, este lugar encontra-se sob vigilância de um circuito fechado de televisão, procedendo-se à gravação de imagem.
REFER
(Dec. Lei nº 35/2004 de 21 de Fevereiro)

Location-focused 'predictive' systems

Location-focused methods of 'predictive' policing are developed to predict where, and often when, a crime will occur to allocate police resources in those locations. The research partners found examples of geographic crime 'prediction' algorithms in all countries of focus: Belgium, France, Germany, and Spain.

Proponents of location-focused 'predictive' policing systems have claimed that data-driven approaches can make policing more efficient. By identifying locations that pose the greatest threats, the argument goes, police can prevent crimes from taking place. This approach has been summarised as follows:

> *"If police can target their resources on these risky people, places, and times, they will be more effective at reducing crime in their jurisdictions".*[44]

In Europe, researchers have identified two main types of location-focused systems:

— crime 'hotspot' prediction algorithms, which draw on historical policing data to forecast future crime locations; and

- ‘risk’ prediction algorithms, which are based on the assumption that environmental factors determine where crimes take place.

Both methods raise concerns about the disproportionate targeting and criminalisation of racially minoritised and low-income people and communities.

Examples outlined in this report demonstrate that location-focused predictive policing can have serious consequences for people living and working in areas labelled as ‘high risk’. They may face increased police surveillance, monitoring, vehicle and identity checks, searches, questioning, and even arrest.

Although the EU AI Act includes a nominal ban on certain types of ‘predictive’ policing systems, per the official guidelines, it does not cover location-focused ‘predictive’ systems.[45] The research makes clear these systems’ potential for discrimination and profiling, They must be included in any meaningful prohibition of predictive policing.

This report only provides a snapshot of the geographic crime ‘prediction’ systems used by police forces across Europe. In addition to the systems in France, Belgium, Germany, and Spain, there are also similar examples in the Italy, Switzerland and the UK — as identified by previous research.

Crime ‘hotspot’ prediction

Location-focused systems in Belgium, France, Germany and Spain predominantly use crime ‘hotspot’ prediction methods. Through this, historical crime statistics that show where and when crimes took place are used to ‘predict’ future crime locations or ‘hotspots’.

Researchers identified at least nine different ‘hotspot’ prediction systems. Many of these are being rolled-out by multiple police forces in each country.

In Germany:

- Berlin police are implementing a strategy for classifying ***kriminalitätsbelastete Orte*** (kbOs) or ‘places affected by crime’, where extended police powers can be used;[46]
- three German federal states are using crime ‘hotspot’ systems, down

from the six states using five different systems in 2018.[47] These systems are:

  - SKALA (***System zur Kriminalitätsauswertung und Lageantizipation***, System for Crime Analysis and Situation Anticipation) in North Rhine-Westphalia;
  - KrimPro (***Kriminalitätsprognose Wohnraumeinbruch***, Crime Forecast for Residential Burglary) in Berlin; and
  - KLB-operativ (***Kriminalitätslagebild***, Crime Situation Awareness) in Hesse;[48] and

- Bavarian police have used the Pre-Crime Observation System (PRECOBS).[49]

Location-focused 'predictive' systems are being used widely in Spain:

- the 'Predictive Police Patrolling Decision Support System (P3-DSS) is used nationally;[50] and
- seven different regions are using a EuroCop system, including nearly all police forces in Madrid.[51]

In France and Belgium, researchers found fewer active examples of 'hotspot' policing methods. In France, ***La Quadrature du Net*** identified 'PredVol' and PAVED, which were both used by the ***Gendarmerie Nationale*** but have since been discontinued.[52]

In Belgium, ***TechnoPolice*** identified a small trial by Westkust police, and the use of the Geographic Information System, produced by the company Orbit, in Flanders and Brussels.[53] Orbit alleges its software is "already in place in nearly 100 police zones".[54]

Crime 'hotspot' prediction systems have received widespread international criticism following scrutiny of the PredPol system in the US for reinforcing and perpetuating racial bias.[55]

The systems covered in this report, some of which use broadly similar methods to PredPol, also raise concerns for discrimination and criminalisation. In all four countries, the areas labelled as 'high risk' by crime 'hotspot' systems are often areas where marginalised communities live and work.

Purposes

Police claim that statistical calculations for crime ‘hotspot’ prediction allow them to reduce crime rates. Florian Gauthier, the French data scientist who designed PredVol, justifies the need for ‘hotspot’ policing for predicting car thefts by pointing out the discrepancies between the places where officers patrol, and the places where car thefts take place. These discrepancies, he implies, can be reduced by using crime data to direct officer patrols.[56]

Allegedly, ‘evidence-based’ methods make it possible to deploy officers to the right place at the right time, deterring criminal activity before it even takes place. In Germany, Berlin police claim that designating an area as a kbO increases the “sense of security”, as it allows police to “control the identity of relevant persons, increase the risk of detection, and thus prevent criminal offences”.[57]

Many of the ‘hotspot’ policing systems identified are for alleged thefts or burglaries:

— in France, PredVol is for alleged car thefts, and PAVED[58] for car theft and burglary;

— in Germany, the PRECOBS system focuses on alleged vehicle theft and burglary, while the KbO system includes a focus on robbery, among other offences;[59] Researchers have suggested that ‘hotspot’ systems for burglaries were introduced in the 2010s as a response to a media panic over burglaries;[60]

— in Belgium, the local Westkust police force ‘predictive’ system focuses on burglary and vehicle theft,[61] and

— in Spain, the EuroCop system attempts to ‘predicts’ thefts, among other offences;[62]

Data used

Crime ‘hotspot’ prediction systems draw statistical insights and trends from large amounts of crime data, often from police databases, to forecast where future crimes will take place.

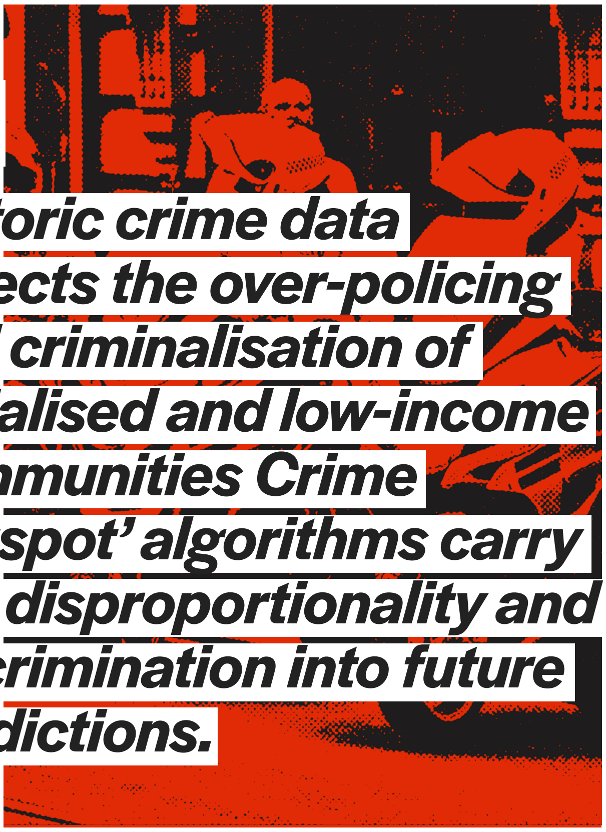
In Germany, the kbO (***Kriminalitätsbelastete Orte***, Places affected by crime) location-focused ‘crime’ prediction model uses a statistical assessment including crime data and other unspecified additional information.[63]

In Belgium, the Orbit Geographic Information System, apparently used by more than 100 local police forces, uses historic police crime reports to identify future crime ‘hotspots’.[64] The Westkust local police force system similarly uses police data on alleged crimes, licence plates, court records, and even the weather.[65]

In France, the PredVol system draws on data about car thefts from the IT systems used to record all complaints and reports, including:

- XY coordinates where the car theft took place;
- date; and
- additional information on the vehicle model and colour.[66]

In Spain, the EuroCop system can draw on and integrate multiple sources of information, including police crime data and files, socio-economic data and video-surveillance data. This is combined in an algorithmic model to ‘predict’ crime, and to generate ‘heat maps’ and ‘patrol routes’ for police.[67]



> ***“Historic crime data reflects the over-policing and criminalisation of racialised and low-income communities Crime ‘hotspot’ algorithms carry this disproportionality and discrimination into future predictions.***

There are serious concerns that historical police data in crime ‘hotspot’ systems will cause unlawful discrimination. As will be explained later, historic crime data reflects the over-policing and criminalisation of racialised and low-income communities. Crime ‘hotspot’ algorithms carry this disproportionality and discrimination into future predictions.

Indeed, the Belgian interior minister acknowledged in June 2020: “Police statistics are first and foremost a reflection of police activity. They do not reflect the reality of crime in a given area.”[68]

Many ‘hotspot’ systems also draw on socio-demographic data in their training datasets. PredVol’s developer told ***La Quadrature du Net*** that the system used 600 sociodemographic variables. These include school attendance and unemployment levels, number of nearby shops, and average population age. The authorities would not provide more comprehensive information.[69] They also found that PAVED, out of 15 socio-demographic variables, drew on gender, nationality and immigration data, household income, and level of education.[70]

The Spanish National Police P3DSS 'Smart Patrolling' system also used nationality data, dividing residents of Madrid into groups: Spanish citizens, other EU citizens, non-EU citizens, and unusually, citizens by continent.[71] The system then calculated for each nationality group a "police contact goal": the amount of patrol time to be allocated to each group based on its size in relation to the geographic territory.[72] These demographic groups, while extremely generalised, are essentially placeholders for racial groups.

Data on nationality, immigration status, and gender are all, or may be considered as, "special categories" of data.[73] These and other sociodemographic variables risk establishing correlations between criminality and race or economic deprivation. EU data protection law makes clear that:

> *"Profiling that results in discrimination against natural persons on the basis of personal data which are by their nature particularly sensitive in relation to fundamental rights and freedoms should be prohibited".*[74]

Based on this input data, 'hotspot' systems use statistical analyses to forecast the probability of future crime locations. The specific modelling techniques to conduct these geographic and temporal analyses differ from system to system.

PAVED and PredVol use machine learning techniques, meaning the systems automatically 'learn' from additional data, without needing to be manually retrained. Most other 'hotspot' systems identified in Belgium, France, Germany and Spain use algorithmic methods.

Outcomes

Generally, 'hotspot' prediction systems provide police with a 'heat map' forecasting areas or locations where there is allegedly a high risk of crime taking place. For example, PRECOBS in Germany displays a map with areas marked in different colours. These represent the supposed probability, or risk levels, that a crime will occur in that area (see figure 1).

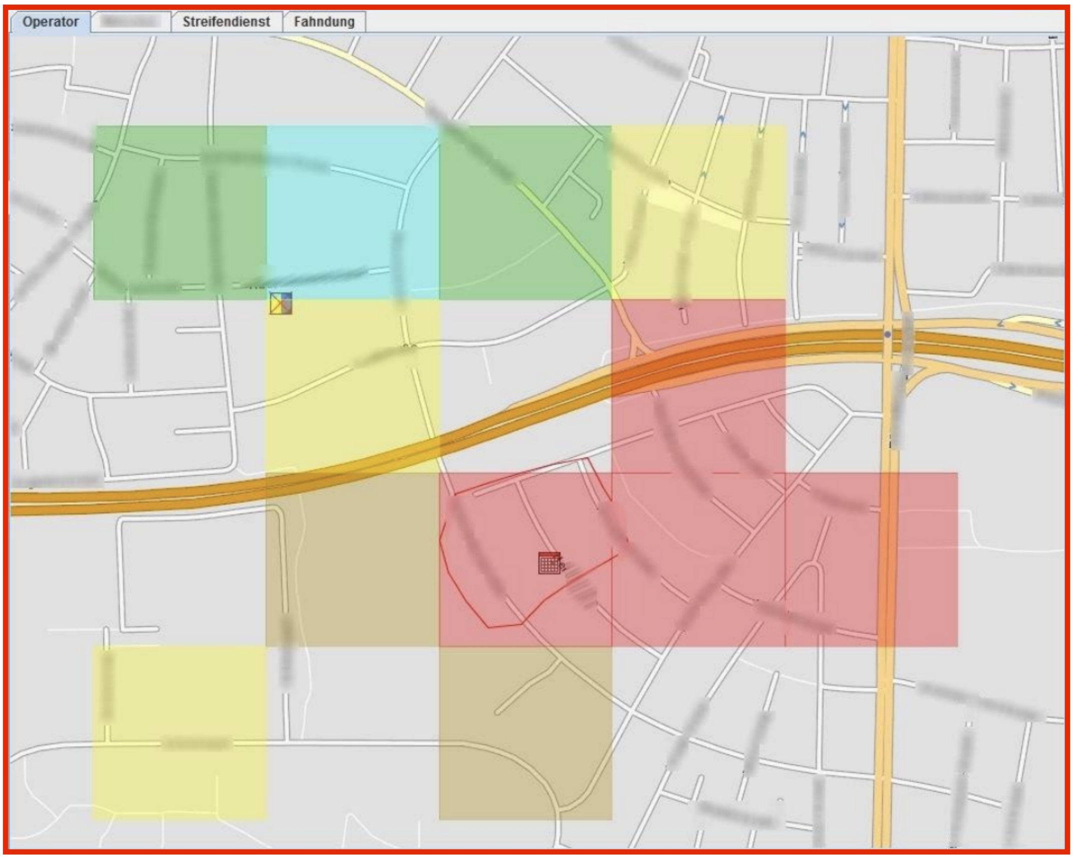
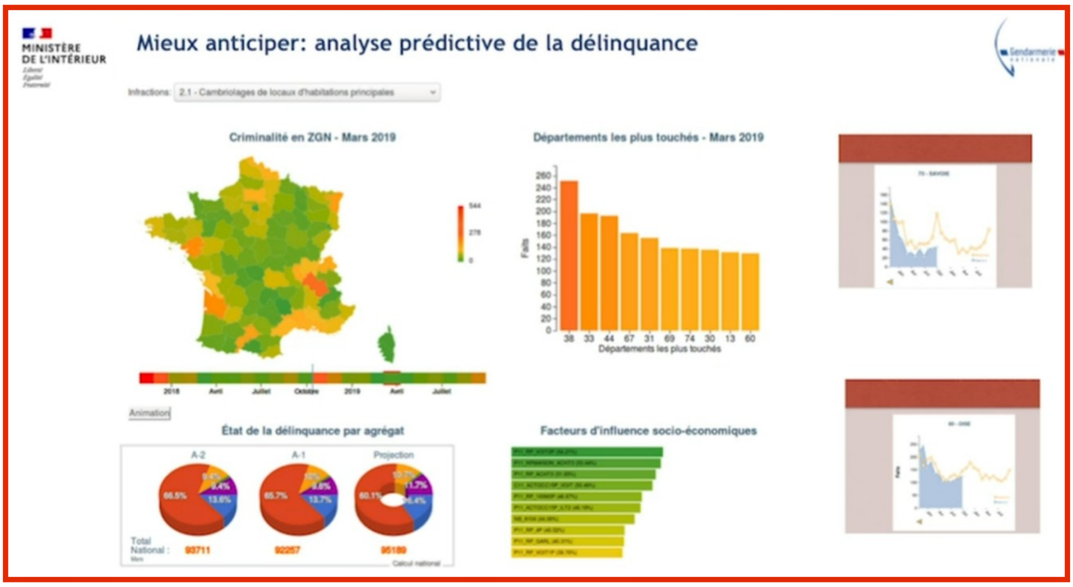


FIGURE 1: A SCREENSHOT OF THE PRECOBS COLOUR-CODED MAPPING ON A LOCATION. CREDIT: SONJA PETERANDERL

Some systems, such as PredVol in France, are accessible 'in the field' for officers to view on tablets. Other systems, such as PAVED, are accessible only to commanders. In addition to 'heat maps', PAVED also presents officers with histograms displaying the socio-demographic variables considered the most influential indicators of criminality (see figure 2).


MINISTÈRE DE L'INTÉRIEUR

Mieux anticiper: analyse prédictive de la délinquance

Infractions: 2.1 - Cambriolages de locaux d'habitations principales

FIGURE 2: SCREENSHOT OF THE LECTURE GIVEN BY COLONEL PATRICK PERROT, COLLOQUE DE L'INSTITUT DE DROIT PRIVÉ—UT CAPITOLE—SEPTEMBER 8, 2021 (SOURCE: "AI ET ENJEUX DE SÉCURITÉ," AT 23M10S).

Crime 'hotspot' prediction systems are used to allocate police resources and determine where and when officers should patrol. Outcomes in 'hotspot' areas may include:

— surveillance;

— information-gathering;

— identity checks;

— questioning;

— searches;

— restraining orders; or

— arrests.[75]

The designation of 'hotspot' areas may also allow for extended police powers in those locations. In Berlin, police are legally allowed to carry out identity checks or searches of people or objects in so-called 'kbOs' without concrete suspicion, instead "depending on behaviour".[76]

Similarly, ***La Quadrature du Net*** spoke to one source who explained that 'hotspots' generated by PAVED were used to persuade prosecutors to issue special warrants for identity and vehicle checks in those locations. These allowed administrative police to use judicial police powers – a serious violation of administrative police duties.[77]

Impacts

Locations labelled as crime ‘hotspots’ by algorithmic systems are disproportionately areas or neighbourhoods where low-income and racialised communities live and work. Legal expert Lina Schmid points out that places classified as ‘kbOs’ are usually frequented by a high proportion of people perceived as migrants.[78]

Following the introduction of the PRECOBS system in Bavaria, Matthias Monroy, the editor of the German civil rights journal ***Bürgerrechte & Polizei*** (***Civil Rights & Policing***) said:

> ***“Who do police stop more often when they assume that a burglary is imminent in the next few hours or days? I’d say it’s more likely to be people in scruffy clothes, people of a different skin colour, or in hoodies — patterns that already exist among police.”***[79]

In Germany, checks carried out by the police on the basis of racial attribution are constitutionally prohibited (Article 3 of the ***Grundgesetz*** or Basic Law). However, Lina Schmid explains that designating certain areas as crime ‘hotspots’ allows police to circumvent this ban:

> ***“Criminalised here - instead of racialised groups of people, as is usual with racial profiling - are entire places and the people who frequent these places. This opens up space for the police to carry out racial profiling in a hidden manner, because: even if all people are supposedly checked… in practice, however, it is still primarily BIPoC [Black, Indigenous and People of Colour] that are targeted by the police.”***[80]

The residents’ initiative ***Wrangelkiez United*** have said that the checks in the Görlitzer Park/Wrangelkiez kbO almost exclusively affect Black people and racially minoritised people, “regardless of what they are doing or where they are going.”[81] Students at a language school in the neighbourhood are checked on their way to class, and Black men regularly experience controls in the park, as reported in video interviews with ***Wrangelkiez United***:

> ***“When the police are present (…) then dark-skinned people like me are checked for no real reason – it’s not that we’ve committed any offences. It’s because of what we look like.”***[82]

Environmental ‘risk’ prediction

Location-focused systems in Europe also include ‘risk’ prediction systems which draw on environmental or contextual data to identify locations allegedly more prone to criminality.

These environmental ‘risk’ prediction systems are underpinned by the ‘broken windows’ criminological theory. This argues that the physical environment is a determining factor of crime. It was introduced by James Wilson and George Kelling in the US in 1982.[83] The theory builds assumptions around environmental factors (such as broken windows) as indicators or deterrents of criminality.

‘Broken windows’ policing was subsequently introduced across policing in the US. An oft-cited example are changes introduced by former New York Police Department commissioner William Bratton.[84] It has since informed the design and development of data-driven policing methods, despite being largely discredited by criminologists and sociologists.[85]

As with crime ‘hotspot’ algorithms, environmental ‘risk’ algorithms may direct police to areas in cities that are more economically deprived, and more likely to be inhabited and frequented by racialised communities.

Purposes

Belgian and French police forces are using an algorithmic model called ‘Risk Terrain Modelling’ to predict crime or criminality, which includes assessing environmental ‘risk’. There are other known uses by police in the UK.[86]

The Risk Terrain Modelling (RTM) methodology was developed by Joel Caplan and Leslie Kennedy, two academics at Rutgers University in New Jersey, US. It has allegedly been tested in over 45 countries across six continents. The Risk Terrain Modelling website, which advertises the software produced by the company Simsi, states:

> *“What risk terrain modeling (RTM) does is to identify the risks that come from features of a landscape and model how they co-locate to create unique behavior settings for crime.*
>
> *You can probably imagine the clichéd “dark alleyway” when thinking of potential locations for criminal activity. In this case, you are considering at least two attributes of a landscape: (1) an alleyway*

> *and (2) poor lighting. The risk of crime is thought to be exceptionally high at places where these particular attributes coexist.”*[87]

The website distinguishes Risk Terrain Modelling from crime ‘hotspot’ prediction methods, saying:

> *“Hotspots tell you where crime is clustering, but not necessarily why. All too often people focus on hotspots without giving equal consideration to the spatial attributes that make these areas opportunistic in the first place... Hotspots are merely signs and symptoms of places that are highly suitable for crime. RTM advances this by providing the spatial diagnosis.”*[88]

Risk Terrain Modelling is currently used in Zennevallei (Belgium) and Paris (France). The ***Direction de la Sécurité de Proximité de l’Agglomération Parisienne*** (DSPAP, or the Paris Region Local Security Division) started using the algorithm after a geo-statistician at the former ***Observatoire National de la Délinquance et des Réponses Pénales*** (ONDRP, or National Observatory of Criminality and Penal Responses)[89] worked for several years with Rutgers University, saying:

> *“I have been using the RTM (Risk Terrain Modelling) algorithm for over eight years... It is now a web application, much more powerful than it previously was, but it uses the same principle: it’s in line with situational crime prevention, meaning that we identify the contextual and environmental elements that make crime happen... So by analysing an environment and identifying the factors that aggravate risk, we can predict what might happen in a similar environment.”*[90]

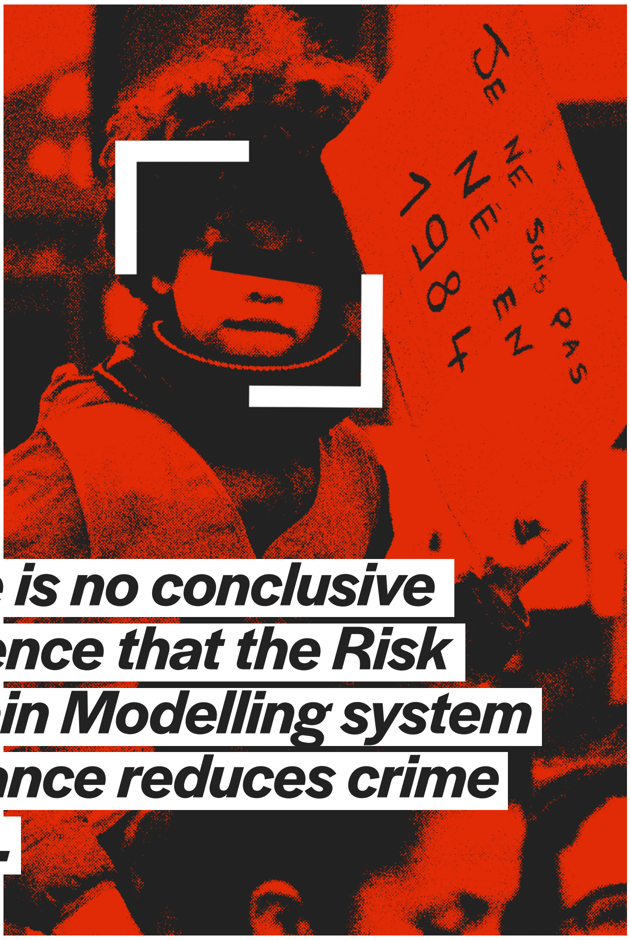
In Zennevallei it is used for similar purposes. Here, the programme was spearheaded by Anneleen Rummens, a doctoral student from Ghent University, under the supervision of criminology professor Wim Hardyns.[91]

There are other environmental ‘risk’ prediction systems that do not use the Risk Terrain Modelling algorithm. These include MapRevelation and the ‘predictive module’ of the Smart Police system in France. MapRevelation was one of the first ‘predictive’ policing systems deployed in France. Marketed by the company Sûreté Globale,[92] it is used by local authorities and municipal police forces in Montpellier, Lyon, Lille, Villeurbanne, Montauban, Angers, Colombes and Melun Val de Seine.[93]

Data used

The Risk Terrain Modelling system draws on various 'weighting factors' that are fed into the final model. These factors can be adjusted according to the specific use case of the model. The algorithm assigns a vulnerability value to locations based on spatial factors, including:

- whether the location is well-lit;
- metro or bus stations;
- outdoor seating areas of cafés;
- fast-food outlets;
- public toilets;
- pharmacies;
- grocery stores;
- bars;
- trees and benches;
- certain types of shops;
- schools;
- post offices.



> **“**
> ***there is no conclusive evidence that the Risk Terrain Modelling system in France reduces crime rates.***

On the Risk Terrain Modelling website, examples of other factors include: 'drugs', 'vacant', and 'gangs'.[94]

In Paris, the Risk Terrain Modelling system draws on data from the Police National Procedure Writing Software (LRPPN, or ***Logiciel de Rédaction des Procédures de la Police Nationale***). It deduces correlations between acts of crime and so-called environmental factors. In 2018, Jean-Luc Besson, head of the ONDRP's geo-statistical department gave an insight into which factors may be used in the Paris model:

> *“If we look at pickpocketing near cash machines, we'll ask ourselves: are the most affected cash machines open day and night? Are they near a crossroads or a train station, etc.?”*[95]

Researchers were unable to obtain precise information on all the variables used in the Paris and Zennevallei Risk Terrain Modelling systems. However, it is known that the Zennevallei model uses factors such as weather conditions during specific events.[96]

In France, MapRevelation has allegedly been trained on a ‘terrorism’ database, with the aim of ‘predicting’ attacks.[97] It is also fed with data held by the municipal police forces that use the system.

The ‘predictive module’ of Smart Police, developed by the French company Edicia, uses machine learning techniques. It draws on both operational police data (e.g. reports, offences, location of officers and vehicles) and urban data (e.g. environmental and weather data, national and local events, socio-demographic and electoral data).

The ‘predictive’ module of Smart Police also allegedly draws on information from social media and other partners. These include high school principals and social housing landlords, as well first-hand knowledge from police officers.[98] This holds obvious risks of encoding rumours, hearsay, and unverified opinions into algorithmic systems, disguising them with a veneer of technical objectivity.

Outcomes

A culture of secrecy in police forces and government bodies made it difficult to find conclusive information on the outcomes of environmental ‘risk’ prediction systems used in Belgium and France.

According to a source contacted by ***La Quadrature du Net***, there is no conclusive evidence that the Risk Terrain Modelling system in France reduces crime rates. The source also indicated that the Risk Terrain Modelling methodology allows institutions using it to evade reflection on the structural causes of crime.[99] A similar issue arises with other crime ‘hotspot’ prediction systems.

Other location-focused crime ‘prediction’ systems in use in Europe

In addition to the systems detailed above in Belgium, France, Germany and Spain, other police forces across Europe are also using location-focused ‘predictive’ policing systems.

In the UK, ***Amnesty International UK*** recently found that almost three-quarters of police forces were using ‘predictive’ policing systems, with

32 out of 46 forces using location-focused crime 'prediction' systems.[100] ***Amnesty*** investigated the use of Risk Terrain Modelling by UK police forces and found that the use of Risk Terrain Modelling by London's Metropolitan Police "contributes to and reinforces racial profiling and discriminatory policing".[101] Demographic analyses of the areas labelled as 'high risk' by the Risk Terrain Modelling algorithm showed that:

> *"...the areas where the risk terrain modelling system predicted serious violence would occur correspond significantly with the areas with a higher population of deprived Black African, Black Caribbean, Asian Bangladeshi and Asian Pakistani residents."*[102]

Reflecting on the use of environmental 'risk' factors for 'predicting' crime, Dr Adam Elliott-Cooper, an academic and author of ***Black Resistance to British Policing***, said:

> *"[W]e should be unsurprised that the kind of built environment which is targeted by the police will not be semi-detached houses with a white picket fence. They'll be council estates, it will be inner city urban areas which are overpoliced, not wealthy suburban areas, right? So we'll see the ways in which this purportedly geographical approach and thus purportedly more scientific and objective approach to policing, is in fact simply reproducing these existing problems".*[103]

In the Netherlands, police have been using the 'Crime Anticipation System'. This 'hotspot' prediction system originally drew on data points, such as how many 'non-Western' individuals with at least one foreign-born parent were living in an area. Although these data points were later removed, the system continued to use historic crime data and proxies for race and class, such as income and benefits data.[104]

The Italian police previously used 'Delia', a system developed by a company called KeyCrime. This has both geographic and individual crime 'prediction' functions. It is allegedly one of the first examples of commercially available 'predictive' policing software in the world, becoming operational as early as 2008.[105] However, KeyCrime has since gone into liquidation, with the blaming financial uncertainty caused by the introduction of the EU's AI Act, and the possibility that the system may be prohibited in future.[106]

A system called XLAW continues to be used in Italy, however.[107] XLAW is an environmental 'risk' prediction system — similar to the Risk Terrain

Modelling systems used in France, Belgium, and the UK. The system's spatio-temporal predictors include: large venues, month-end pension payments, shops' closing hours, train and ship arrivals, and weather variations.[108]

In some cantons in Switzerland, police have been using PRECOBS — the same system that is used in Germany.[109]

Person-focused crime ‘prediction’ and profiling systems

Person-focused crime ‘prediction’ tools are designed to predict a person’s likelihood or ‘risk’ of committing certain actions, in particular those defined by law as criminal offences. Rather than focusing on a particular location, they focus on particular individuals.

Police and criminal legal system authorities are using these systems to attempt to profile, ‘predict’ or assess the ‘risk’ of a person committing a criminal offence or carrying out criminalised behaviour. Other such systems try to assess the likelihood that someone may become a victim of crime, such as gender-based violence. They have also been used to try to detect allegedly false crime reports.

People targeted by these systems are subjected to analysis of data that characterises them, their past and present lives and their relationships. The objective is to determine and ‘predict’ their behaviour, ‘risk’, or supposed ‘criminality’.

This can lead to potentially serious consequences. These systems may lead to people being put under surveillance or monitoring. They may face increased police stops, questioning, searches, home or workplace visits. The use of these systems can even lead to detention, arrest, or deportation.

These systems are also used in the criminal legal system. They can influence judges' decision-making, for example on sentencing. They may influence the length of a person's imprisonment, when they will be released, and the conditions in which they are held.

Purpose

Person-focused 'predictive', profiling and 'risk' assessment systems are being used for a wide range of different purposes. Some forces use data mining and analysis software to collect and collate data, assess patterns, and use these to 'predict' future patterns.

In Germany, three federal states hold licences for 'big data' mining and analysis programmes based on the Gotham software developed by US technology company Palantir. Like many other corporations that develop and sell police technology, Palantir is very secretive about both the technology and the contracts it signs.

Hesse State Police in Germany use a Palantir-powered system called ***hessenDATA*** to create extensive individual profiles on people. The system can show a record of known information about a person, including: when and where they have been stopped by police, record of arrests, whether they have ever been caught with drugs, and where they live.

In Belgium, a system used by the Belgian National Police called 'i-Police' has multiple functions, including:

- analysis and 'prediction' of patterns;
- predicting future crime for the purpose of 'prevention';
- enabling monitoring and surveillance;
- the allocation of police patrols, stops and checks;
- and other forms of intervention and enforcement.[110]

Belgian police also profile people and groups and put them on specific databases, an issue considered in more depth below. This includes the use of these databases for so called 'urban gangs', a term laden with racism.[111] People profiled as alleged 'gang' members have been targeted for monitoring, surveillance and increased stop and search.[112]

Individual crime ‘prediction’, profiling and ‘risk’ assessment tools have been introduced in Germany to assess the alleged future risk posed by so-called Islamist[113] terrorists or terrorism supporters. The Federal Criminal Police Office has developed two individual ‘risk’ assessment tools called RADAR (‘Rule-based Analysis of Potentially Destructive Offenders for the Assessment of Acute Risk’).

One iteration, RADAR-iTE is a tool used to analyse and profile so-called ‘Islamists’. Belgium’s Federal Police have also said they use a similar tool to RADAR-iTE.[114] The other, RADAR-rechts, is used by the German Federal Criminal Police Office to profile people with right-wing views who are considered a violent threat. The authority is also developing a further tool, RADAR-Haft (“RADAR-detention”) to assess the propensity for violence posed by imprisoned people upon release.

RADAR-iTE and RADAR-rechts are intended to evaluate mainly the risk of those previously identified as “Gefährder” (endangerer). This is a threat classification developed by German law enforcement authorities that has now been exported throughout the EU.[115] The term is ill-defined and open to subjective interpretation. The systems are also used to assess “relevant persons,” another ill-defined and subjective category. The risk profiling is used to assess and prioritise ‘high-risk’ individuals for subsequent enforcement and intervention.[116]

In Spain, VioGén is one of the most well-known individual risk assessment systems. Its purpose is to assess the risk of gender-based violence to an individual who has reported an incident. The assessment determines the actions police take as a result.[117]

A more unusual type of ‘predictive’ system has also been used by police in Spain. VeriPol is an algorithmic system used by the Spanish National Police to detect allegedly false crime reports. It uses natural language processing techniques to scan the texts of reports on robbery, pickpocketing and purse snatching. It is effectively used as a lie detector. It was created to prevent fraud resulting from false reports. The main aim is to provide officers with a quick evaluation on whether or not a crime report is potentially false.[118] In March 2025, it was reported that the National Police had stopped using VeriPol. The Spanish Ministry of the Interior said this was because the system lacked validity in judicial proceedings.[119]

Security authorities worldwide, including in Europe, are increasingly analysing so-called 'passenger name records' (PNR). This is personal data collected by airlines for business purposes when a person books a flights.[120] PNR data is cross-checked with police and other state databases. Algorithms are used to systematically search for patterns in this data according to predetermined criteria.[121] Systems such as these effectively turn the presumption of innocence on their head, making anyone travelling by air into a suspect.[122] The EU is planning to extend their use to other forms of transport, beginning with maritime travel.[123]

In Spanish prisons, a system called DRAVY is used to try to identify prisoners allegedly undergoing a process of so-called 'jihadist' radicalisation.[124] As the main purpose of DRAVY is for assessing 'jihadist' radicalisation, it is fundamentally discriminatory on the basis that it is almost exclusively focused on Muslims and people from Muslim backgrounds. The system is set up to target 'jihadism', a term that itself relies on discriminatory Western stereotypes.

A similar tool called RisCanvi is also used in Spanish prisons, to 'predict' the risk of people re-offending. It is used to make decisions on parole, temporary release, and prisoner categorisation.[125]

Data used

These systems are trained, developed and operated using data from police, law enforcement and criminal legal system authorities.

These authorities often collect or access data from a wide range of sources. In Germany, Palantir's systems use data from police databases and other sources, including social media. In recent years legal challenges have been brought against the systems, as well as against the data analysis laws underpinning their use.[126] When one legal challenge successfully restricted the scope of analyses and data sources, a German police source said: "There was a groan when the verdict came and colleagues realised that they were no longer allowed to do so much".[127]

The Belgian i-Police system aims to incorporate data from all Belgium police databases and video surveillance footage. It also uses open-source 'intelligence', such as social media information and press reports. To fulfil these functions, i-Police deploys digital technologies from a range of subcontractors, including a number of Israeli companies such as

Interionet and TA9/Rayzone. The latter's CEO formerly served as Deputy Director of Unit 8200, the intelligence unit of the Israeli military, which is responsible for developing and deploying 'Gospel', an AI system for automatically generating bombing targets in Gaza, as part of Israel's ongoing genocide and mass killing of Palestinians.[128]

The data used by these systems is fundamentally biased. Police across Europe disproportionately target people from minoritised ethnic backgrounds. For example, police in Spain disproportionately stop and search people based on their racial, ethnic, or religious appearance.[129] In Germany, non-citizens are overrepresented among suspects recorded by the police, those convicted by the courts and those imprisoned.[130] The Belgian criminal justice system has been condemned on several occasions for its racist practices, particularly ethnic profiling.[131] The UN Committee on the Elimination of Racial Discrimination (CERD) has shared concerns that people with foreign backgrounds are overrepresented in the Belgian criminal justice system, especially in prison.[132]

> **"*The data used by these systems is fundamentally biased.***

The police and criminal legal system data used in these digital systems is riddled with structural and institutional biases, over-representations and discrimination. Yet it is used to create, develop and operate data-based 'predictive', profiling and 'risk assessment' systems. This leads to increased targeting of the same marginalised groups and communities. The results of these operations will then be fed back into the systems, increasing the probability that people from those groups and communities will be perceived as 'high risk' in the future. In this way, these algorithms produce a self-fulfilling prophecy or feedback loop. There are clear examples of how this discriminatory data influences the outputs of these systems.

The full list of data used by the German RADAR-iTE profiling system is not known. However, it relies upon remote assessment without any direct contact with the individual being assessed.[133] The assessment includes topics such as "violence against people," "interaction with authorities and other institutions" and "military and travels." Other questions include: "What is his private life like? Is the person more of a loner or does he operate in a group? Does he have contacts outside the Islamist scene? Does he have a job?”.[134]

These kinds of profiling points mean that someone who has travelled from a conflict zone, or who uses certain routes for tourism or for family visits, may be profiled as suspicious or a ‘risk’. Data points such as associates, contacts or travel patterns can clearly lead to discrimination.[135] The RADAR-iTE assessment also contains other concerning and potentially discriminatory elements on mental health problems and suicidal tendencies.[136]

There were also issues with the data used to train the now-discontinued Spanish VeriPol system, used to detect false crime reports. VeriPol was trained on reports submitted to the police, which were manually catalogued by an officer as false or real. However, not all of those cases had been resolved, and so there was no objective or conclusive finding of truth or falsehood. The model was therefore built entirely using assumptions made by the police officer who catalogued the reports.[137] It is remarkable that it took at least seven years for the Spanish authorities to recognise the problems with the system and halt its use.

The VioGén system in Spain allegedly predicts whether someone will experience gender-based violence. However, the system did not use the actual testimonies of the women who reported cases of gender-based violence, but police officers’ reports of the women’s accounts. The resulting risk score is thus entirely dependent on the assessment of the police officer.[138] The system can also only process data from reports that are actually filed.

However, many experiences of gender-based violence go unreported, particularly those of migrant women, women from marginalised and more deprived backgrounds, and women with children. Along with LGBTQIA+ people and people with disabilities, these groups are the most affected by structural difficulties in reporting their aggressors. The system therefore did not fully account for the experiences of those most marginalised in society.[139]

The concepts underpinning these ‘predictive’, profiling and ‘risk’ assessment systems are also fundamentally biased. This problem stems from a lack of clarity that leads to subjectivity, or culturally specific terms with racialised undertones.

In Germany, vague terms such as “Gefährder” (endangerer) and “relevante Person” (persons who may play an important role) are used to categorise persons suspected of committing or supporting violence. They have become established working terminology among security authorities and police, and are applied in the RADAR systems. They are not legally defined, and are vague and unscientific. This means people will be profiled subjectively, at the discretion of the authorities, and inconsistently. This undermines the entire legitimacy of the system.

These problems are laid bare by the practical use of the terms. German police forces have been much more hesitant to categorise right-wing extremists as dangerous than so-called 'Islamists'. For example, when a terrorist neo-Nazi organisation NSU (National Socialist Underground) was uncovered in 2011, only four members of the group were categorised as "Gefährder".[140]

There are other issues with the data that is used in these systems. The Belgian i-Police system will bring together data from multiple police sources, including 'non-validated' information. This includes uncorroborated information from police reports, often known or described as police 'intelligence', which includes information on people who have not been convicted or charged with a crime. The chair of the data protection authority that oversees the Belgian police, the COC, has raised serious concerns about this data being used in the i-Police system.[141]

Systems that assess potential criminality, future criminality, or 'risk' of criminality mark a conceptual shift from assessments based on actual evidence of an action or involvement in an action, to an unspecified, abstract risk that ***could*** develop in the future, often estimated only on the basis of circumstantial evidence. This is true for all individual or person-focused systems.

Outcomes and impact

These ‘predictive’, profiling and ‘risk’ assessment systems are used to influence a range of policing and law enforcement decisions and outcomes, from surveillance and monitoring, to stops and questioning, stop and search, home raids and can even lead to arrest.

The German Hesse state police system hessenDATA facilitates incredibly invasive surveillance. Despite its supposed use for ‘serious’, ‘organised’ or ‘state security’ crime, it has been used extensively for non-violent crimes. In 2022, it was reported that police categorised around 12,000 of the 14,000 hessenDATA queries per year as ‘preventive measures’ against criminal offences.[142]

The outputs from these systems generally assign people with a ‘risk’ score: low, medium or high, or variations on those categories. This signals their supposed likelihood of committing an offence or criminalised behaviour.

According to Germany’s Federal Criminal Police Office, around 800 people from the ‘Islamist’ spectrum have been assessed by RADAR-iTE since 2017.[143] As of November 2023, 487 people were classified as dangerous (***Gefährder***) in relation to ‘politically-motivated’ crime underpinned by religious ideology. In contrast, the number of right-wing people categorised as ***“Gefährder***” or “relevant person” is still relatively low – as is the number of RADAR-rechts assessments.[144]

The VioGén system used by Spanish police is used to assign risk scores, but for victims, not offenders. A low score means that the police will check on the victim through phone calls, for example, while an extreme risk score may mean that the police will monitor the victim’s home or assign security patrols to ensure their safety.[145] In 95% of cases, police officers follow what the VioGén risk score tells them.[146]

As a result of Passenger Name Record (PNR) profiling, the German Federal Criminal Police Office cited routes between Turkey and Germany as potentially suspicious routes. They are allegedly often used by ‘Islamist’ terrorists “as they are also popular with tourists and therefore offer cheap prices and good camouflage opportunities”.[147]

The DRAVY system used in Spanish prisons incorrectly predicts a high level of risk for almost half the people it assesses.[148] This results in those people receiving stricter treatment and tougher living conditions in prison.

Non-Spanish nationals are disproportionately targeted.[149] The RisCanvi system, also used in Spain, is also known to discriminate on the basis of socio-economic status or by association with others. It gives higher risk scores to people with a history of 'unstable' employment and finances, those without family or social support, and to people who have family members or parents with a criminal history.[150]

The extent of people targeted by this profiling, and the consequences, are significant.

The extent of people targeted by this profiling, and the consequences, are significant.

By September 2023, the VioGén system had assessed around 770,000 cases.[151] Millions of air passengers are profiled through Passenger Name Record (PNR) systems. In 2022, 156 airlines in Germany transmitted around 424 million PNR data records to the police, covering some 121 million passengers. In 2023, around 385 million PNR records were generated by 31 October, relating to 107 million passengers.

In addition, beyond violating the privacy of tens of millions of people, PNR systems have led to substantial numbers of people facing police interventions. In 2023, more than 10,000 actions were taken by German police on the basis of PNR profiling. Almost a fifth of these were found to be false positives (an incorrect match).[152] In the 8,284 cases of true positives (correct matches), the following measures were implemented:

— 2,178 residency investigations;

— 2,394 police observation/covert controls;

— 1,236 arrests, 2,303 targeted (open) checks; and

— 173 rejections/refusals of entry.[153]

Millions of passenger data records are thus analysed in order to carry out several thousand criminal or immigration investigations, the objective evidential basis of which is non-existent, or extremely tenuous.

Individual cases highlighted in the report on Germany illustrate the extreme consequences of being (incorrectly) labelled as a '***Gefährder***'. Anti-Muslim bias leads to the police and authorities treating Muslim youths differently from white young men with similar problematic behaviour, so they are more quickly considered a threat.[154]

The consequences of being profiled by the RADAR-iTE system include:

— being put under surveillance and monitoring;[155]

— 'preventive detention' ranging in length from several days up to months;[156]

— detention in advance of deportation.[157] and then deportation.[158]

People profiled can also have their asylum claims paused.[159]

Other person-focused crime 'prediction' systems used in Europe

In addition to the examples outlined above, police and criminal legal system authorities in other countries in Europe are also using person-focused crime 'prediction' and profiling tools. Previous research has found evidence of similar systems in police forces and prisons in the UK, Italy, and the Netherlands.

Amnesty International UK recently revealed that 11 police forces in the UK were using used person-focused or individual crime 'prediction' and profiling tools.[160] This includes:

— London Metropolitan Police's 'Violence Harm Assessment' which profiles individuals across London for risk of violence. As of August 2024, 66% of people profiled by the system were Black, whereas only 22%

were white;

- West Midlands Police’s ‘Integrated Offender Management’ system (IOM) for ‘predicting’ individuals’ potential for causing future harm. The force’s internal analysis showed that Black people are 2.4 times more likely to be in the ‘predicted’ high harm group than a north European (white) person.

Across England and Wales, prison and probation services are using the Offender Assessment System (OASys) to ‘predict’ the risk of reoffending for everybody entering the criminal justice system. This system has been widely criticised for racial profiling, privacy threats, and lacking opportunities for accountability or redress.[161]

In the Netherlands, police have used a system called ProKid, which aims to ‘predict’ the risk of re-offending for children and young people.[162] In Amsterdam, police have used two profiling tools called the Top400 and Top600, which attempt to profile the ‘top 600’ and ‘top 400’ young people who are allegedly most likely to commit different types of crime.[163]

Diana Sardjoe, a mother whose sons were profiled by Top400 and Top600, has said that the systems resulted in her sons being continually monitored and harassed by the plans, and called for ‘predictive’ policing systems to be banned.[164]

In Italy, police have also previously used a profiling system called Delia, that included ethnicity data for profiling individuals.[165]

AI video surveillance systems

Increasingly, police forces across Europe are using AI video surveillance systems. These systems use AI-based methods to search through video footage, such as from CCTV cameras and police databases, to identify people and objects, or to detect 'suspicious' behaviour.

The research underpinning this report includes examples of AI video surveillance systems used by police forces in Belgium and Spain. ***La Quadrature du Net*** have separately conducted extensive research on police uses of AI video surveillance in France.[166] In Germany, ***AlgorithmWatch*** identified two pilot projects for AI video surveillance systems in prisons for 'suicide prevention'. There is also evidence of AI video surveillance being used by police in Italy.

The use of AI video surveillance by law enforcement authorities raises significant concerns for infringements on fundamental rights, including the rights to privacy and non-discrimination.

Policing

In Spain, several localities in Madrid use video surveillance systems that incorporate AI methods for image recognition. The systems, provided by Bosch Security through the US-based firm Intelligent Security Services, serves two purposes: automatic number plate recognition (ANPR); and the identification of criminal suspects.[167] The system can also be used to search for people, based on features such as hair colour, clothing, facial features, and their age. There is no concrete evidence to show that the system decreases crime rates. [168] In Madrid, as of January 2025, there are at least 83 AI surveillance cameras, operated by the Municipal Police, with plans to install another 38.[169]

In Belgium, local police forces and the federal police use several AI video surveillance systems. This includes software produced by BriefCam, an Israeli company, for retrospective image analysis by producing video synopses.[170] Like the Bosch system in Spain, this system allows police to categorise people according to criteria such as clothing colour, gender, or belongings.

This latter feature may be unlawful. The Belgian legal framework on non-discrimination allows for targeted research based on objective criteria, but forbids the mass sorting of individuals. Based on these examples and others, the Belgian report calls for the prospective plans for AI video surveillance in the enormous i-Police project to be dropped.

In 2023, France became the first European country to legalize biometric surveillance, in the form of algorithmic video-surveillance cameras, under a law on the organisation of the 2024 Paris Olympic Games.[171] The system was deployed in Saint-Denis, a suburb with a largely minoritised ethnic and working-class population in the north of Paris, where much of the Olympic Games was held.[172] The system was originally legislated for until the end of 2024 – but as soon as the Olympics ended, authorities sought to extend its use.[173]

Elsewhere in France, ***La Quadrature du Net*** has waged a three-year legal challenge against the implementation of Briefcam AI-powered video surveillance software in Moirans, in the Isère region. On 30 January 2025, a court ruled that the usage of this system was unlawful: it violated multiple privacy protections under EU data protection law and the French Internal Security Code.[174]

The ruling invalidates legal frameworks that had previously permitted automated video surveillance systems, including those introduced through temporary experimental authorisations issued for the 2024 Paris Olympic Games. The ruling also set an important legal precedent for ongoing challenges against algorithmic systems used by police in France.[175]

Prisons

In Germany, ***AlgorithmWatch*** identified two pilot projects on AI video surveillance for 'suicide prevention' in prisons. These dystopian surveillance systems would augment existing video surveillance in prison cells with machine-learning algorithms, to try to detect early signs of suicide attempts.

In North Rhine-Westphalia, the Ministry of Justice and German IT company FusionSystems sought to develop a machine learning algorithm based on training footage created by actors. The algorithm was trained to detect objects (e.g. knives, scissors, ropes, lighters) and behaviour that may indicate suicidal intentions. This would include, for example, forming a noose from a belt, knotting a rope or tying a noose to the window grill, pulling out a knife or playing around with a large knife. The algorithm was also trained with footage of inconspicuous behaviour such as squatting, reading, or watching television. This was supposed to teach the system to distinguish between harmless situations and indications of suicide risk.[176] The system also allegedly integrated skeleton tracking, which uses sensors and machine learning techniques to track a person's joint and body movements.[177]

These factors would be used to assign a 'danger level' to the situation in the cell, which would be constantly recalculated. Officers in the prison would be informed of the current situation by a visual 'traffic light' alarm system. An acoustic alarm would sound in cases of high 'danger levels', to allow rapid intervention.

In Lower Saxony, the FZI Research Centre for Innovation Technology and the IT security company VOMATEC Innovations have sought to develop a similar system. The aim is to produce "an operational software as a prototype," which will probably first be implemented in a prison in Oldenburg.[178]

Initially, the project set out to apply AI surveillance technology in communal areas, such as outdoors or in leisure spaces. This was supposed to identify, for example, "the transfer of prohibited objects between prisoners".[179] However, this led to heavy criticism from the Lower Saxony data protection authorities.[180] Unlike the system in North-Rhine Westphalia, which was trained on footage of actors, the system in Lower Saxony is being trained on real recordings of suicide attempts and violence in prisons.[181]

There are significant concerns associated with the use of AI-based emotion or body movement analysis systems. The technology is not only scientifically unproven,[182] but also prone to racial or ethnic bias. For example, camera technology may only be calibrated for lighter skin tones. Facial expressions of Black men are more likely to be interpreted as "aggressive" than those of white men.[183] Cultural biases may influence normative understandings of body language or facial expression. Other factors that may influence this technology are poor lighting, or faces obscured or altered by glasses or headscarves.

Given that false negatives may have potentially life-threatening consequences, the prospective use of these systems is extremely concerning. Even if they do function as intended, with adequate accuracy ratings, they are highly invasive,[184] intruding deeply into the privacy of people in prison. A former prisoner interviewed by ***AlgorithmWatch*** stated that truly effective suicide prevention would require the abolition of the prison system:

> *"Prison is not a therapeutic place, it`s not for rehabilitation, it`s for punishment. So there is no help for people who are in need, it`s very depressing and I can see that people cannot pull along for long... There are also other ways to prevent suicide: by therapy and empathy, having communal support, helping people, to find purpose in their lives."*[185]

In Spain in 2023, the justice department started a pilot in Mas d'Enric prison near Tarragona of "facial recognition and video analysis cameras" for "real-time detection of non-verbal expressions and attitudes indicative of illicit behavior". Partially funded by the European Union, it was intended to be extended to other prisons in the region. However, the Catalan government announced in January 2024 that in light of the recently passed AI Act, it would not continue with the project.[186]

> “
> *Inaccurate data may seem innocuous, but it can have serious consequences.*

Databases

Databases often provide the data used in the ‘predictive’, profiling and ‘risk’ assessment systems used by police and criminal legal system authorities. They can also provide the justification or supposed evidential basis for police and law enforcement action. They cover a wide range of population groups and can contain a vast amount of sensitive information ranging from biographic details to fingerprints, photos and criminal history, amongst many other things.

In Belgium, there are several different categories of databases used by police and law enforcement:

— the National General Database is used for police investigations;

— ‘basic’ databases are comprised of police field notes and ‘intelligence’;

— special databases are set up by police for specific purposes such as so-called ‘urban gangs’;

— common databases share data between the police and intelligence agencies for supposed terrorism purposes; and

— technical databases contain collected data automatically, such as that from ANPR cameras.[187]

France's ***Police Nationale*** and ***Gendarmerie*** use a database called TAJ ('Treatment of Criminal Records'), for the day-to-day activities of law enforcement agencies, which French authorities have attempted to interconnect with several other databases.[188] It includes a wide range of information about people suspected of having committed a serious offence, as well as victims of offences.[189] Amongst municipal French police forces, illegal data collection is a common practice.[190]

The ***Police Nationale*** and ***Gendarmerie*** are authorised to use TAJ for ***post-facto*** facial recognition, in the context of judicial investigations. This means that they can take, for example, CCTV footage or photos of suspects, and use them to search the database for matching records. The facial comparison feature is also increasingly used for administrative identity checks. On average, the system is used for this purpose more than 1,600 times daily.[191]

The Spanish police database on foreign nationals, ADEXTTRA, contains an extensive list of background information. This includes:

- nationality;
- marital status;
- profession and work activities;
- property ownership;
- income and revenues;
- information about cohabitation;
- records of conduct, detention and extrajudicial detentions, and criminal history;
- photographs and other images;
- fingerprints; and
- voice samples.[192]

The databases used by police and law enforcement in Europe contain huge amounts of data. The Belgian National General Database contains information about three million people – a quarter of the Belgian population.

In France, the TAJ database contains almost 20 million individual records, and around 10 million facial photographs.[193] The ***Titres électroniques sécurisés*** database (TES, or Secure Electronic Documents), created in 2016 by the Ministry of the Interior, holds information about all applicants of identity cards and passports.[194] Eventually, the French Ministry of the Interior may be able to access the facial image of every person present on French territory.[195] This dovetails neatly with EU plans to compile 'identity data' on every single foreign national present in EU territory and make it available to police and immigration authorities.[196]

Hundreds of municipal French police forces are equipped with 'Smart Police' software, a platform and digital application which they can use to write up reports 'on the move', take photos and describe events, all of which can be added to relevant central databases. Smart Police includes a 'predictive' element, which collates information from a range of sources, combining police crime data and officer location data with socio-economic population data, weather forecasts and 'rumours' from school principals and landlords and even social media, to attempt to 'predict' the risk of criminality occurring [197]

The data held in these databases and the way they are used can have a serious and significant impact. They contain vast quantities of incorrect information, as well as uncorroborated information presented as 'intelligence'.

Inaccurate data may seem innocuous, but it can have serious consequences. For instance, if outdated information is held about an individual on a database, it could lead to them being wrongly arrested. In Spain, migrants have been erroneously detained because their records on databases were not properly updated.[198]

Along with factually correct information, so-called police intelligence can be used in 'predictive' and profiling systems. This influences system outputs, which in turn influences police and law enforcement decisions. This launders uncorroborated information into fact, which then is used against people.

Databases raise significant concerns in relation to unlawful discrimination. They may be discriminatory *per se*, because of the origin and types of data they contain. Their use can also lead to discriminatory practices.[199] Police and criminal legal system databases significantly over-represent the marginalised people, groups and communities that have historically been targeted, policed and punished by state authorities. This includes Black and racialised people and communities, migrants and people from working-class and socio-economically deprived backgrounds and areas, queer people, and people with mental health issues.[200] Several of Germany's federal states have maintained databases including labels such as "junkie," "vagrant," "gypsy," and "contagious", the latter in relation to people with HIV.[201]

An increasing number of employers and authorities use Belgian police databases for security screenings. People of North African and Belgo-Moroccan origin are overrepresented amongst those who fail these screenings. The report on Belgium also recounts the story of a young Muslim man barred from employment because of erroneous information held on a police database.[202]

Local police forces in Belgium are also known to set up databases to target so-called 'urban gangs', a term heavily-determined by racist perceptions of young men. The conception of these groups both as 'urban' and as a 'gang' is due to their ethnicity, and the parameters for inclusion on these databases were vague. Those on the databases were targeted for monitoring, surveillance and increased stop and search.[203]

Local police in Belgium also maintain databases on sex workers. Ostensibly used to 'regulate' the industry, they make it possible to monitor and track the workers. As registration for sex workers is compulsory, this serves to exclude people with irregular or precarious migration status and pushes them away from networks of support and safety.[204]

The Spanish ADEXTTRA database is used to identify migrants and check their status in the country. It facilitates police identity checks on people who are perceived to be 'foreign'. It has been amply-demonstrated that the Spanish police engage in racial profiling.[205]

There are weak restrictions and safeguards around police use of these databases and the information they contain, and enforcement is also equally weak. Police officers who illegally access data or break the requirements or guidelines are often not reported or punished.[206] Data retention periods are also often exceeded, resulting in the effectively indefinite storage of personal and potentially sensitive data without deletion.[207] Police do not remove data which they are legally required to, and there are few or no enforcement mechanisms or penalties when this happens.[208]

Conclusion

This report has summarised the ways in which police and criminal legal system authorities in Europe are developing, using, and operating ‘predictive’ systems, with a particular focus on Belgium, France, Germany and Spain. This includes crime ‘prediction’ and profiling systems, other automated data-based and data-analysis systems. It has also analysed police databases, and ‘AI’ video surveillance systems used by police and prison authorities.

The report demonstrates a clear trend of police forces increasingly implementing ‘predictive’, profiling, and other data-driven decision-making systems. These are often acquired from surveillance tech companies, including companies that have faced criticism for their involvement with the Israeli state.

The usage of crime ‘prediction’ systems raises serious concerns for increased criminalisation, punishment - including punishments outside the criminal legal system - and discrimination against marginalised individuals and communities, especially racialised and economically deprived people.

The report also raises significant concerns over the accuracy of these systems, the lack of transparency and meaningful accountability, and unlawfulness. As such, 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.

Discrimination

Location-focused ‘predictive’ systems do not contain data on specific individuals. However, it is mainly racialised individuals and those from more deprived backgrounds who are subjected to police stops and checks, and any potential consequences, in the areas where crime is ‘predicted’.

The predictions lead to increased policing of those areas and of the people and communities in them. This leads to racial profiling, stops, checks and searches of people in those areas, and subsequently criminalisation. In this way, crime ‘prediction’ tools provide the justification for the racist targeting of certain areas and the people who live in those areas. It also circumvents supposed legal protections against ethnic profiling.

These law enforcement checks, interventions and incidents are then recorded in the databases that feed ‘predictive’ systems. Use of the data for further ‘predictions’ creates a feedback loop where the same areas and profiles are repeatedly targeted, over and over again.

The same issue of biased data leading to biased outputs and perpetuating feedback loops occurs with person-based predictive systems. The Spanish DRAVY system also exhibits a fundamental discrimination in its design: it focuses on the Western concept of so-called ‘jihadist’ radicalisation and therefore is almost exclusively focused on Muslims and people from Muslim backgrounds. It also has a significant false positive rate. Similarly, the RADAR-iTE system in Germany is predicated on islamophobia and a biased conception of whom constitutes a potential ‘threat’. This results in a significant anti-Muslim bias in its outputs and those impacted.

Criminalisation

Under location-focused crime ‘prediction’ systems**,** entire neighbourhoods are labelled as criminal, and crime is ‘predicted’ to occur there at high rates. This leads to increased police presence and targeting with patrols, stop and search and other operations. It also provides justification for effectively ‘suspicionless’ stops, identity checks and searches – the ‘prediction’ provides both the justification and the suspicion. This increases the likelihood of criminalisation of the people and communities who live and work in those areas. This can occur without objective evidence of criminal wrongdoing.

Person-focused systems profile people based on their backgrounds, labelling them either directly as criminal, or indirectly stigmatising them as potentially criminal. These people are then considered and treated as guilty until proven innocent. People have also been linked by profiling systems to others who are themselves profiled as criminal. This casts an incredibly wide net of criminalisation.

Individual ‘predictions’ or profiles can lead to serious criminal justice and non-criminal justice consequences and punishments. As this report has summarised, known consequences include police or law enforcement surveillance and monitoring, visits to homes or workplaces, raids, being barred from employment, questioning, or even arrests and ‘preventive’ detention. People have been subject to investigations of residency status. They have faced border checks and questioning, leading to refusal of entry, had their asylum claims paused or halted, and even been deported. All of this can occur without any objective evidence of criminal wrongdoing: just data-based, algorithmically generated suspicion.

Transparency and accountability

The lack of transparency surrounding the development, training and operational use of these ‘predictive’, profiling and risk assessment systems is a fundamental bar to justice and accountability.

People who have been targeted by police or law enforcement as a result of ‘predictive’ policing or crime ‘prediction’ systems, are often not aware of that fact. The authorities using these systems generally do not provide information on these systems or how they are used. Nor do they notify people that they have been subjected to profiling, prediction or risk assessment, or that the action taken against them was influenced by one. This raises questions about the fairness and impartiality of the systems and the processes that they influence.

Across Europe, legal frameworks do not require meaningful transparency of these systems. The incoming EU AI Act does not provide meaningful transparency requirements in this context. It includes huge exemptions for systems used to detect, prevent, investigate and prosecute criminal offences.

This needs to change. Police and criminal justice authorities must publish the details of any data-based, algorithmic or automated systems they use on a publicly available database or website, including details of the system or software and how it works, the data used, the way the system conducts analyses or creates outputs and what these are used for, as well as the potential consequences.

If an individual or group is subject to any policing or criminal justice consequences as a result of an automated decision-making system or data-based analyses, they must be informed. The police or criminal justice authority must notify the individual and provide them with information about how they can challenge this decision or output. This information must be provided in a format and

manner that is understandable to an individual with no expertise or knowledge on these systems.

Individuals and groups must have clear routes to challenge the outputs or consequences resulting from such an automated decision-making system, with the potential for meaningful redress.

No legal basis and unlawful use

Many of these controversial systems are developed, tested or operated without a sufficient legal basis for their use. In many cases, they operate without a legal basis, and in some cases have been found unlawful, as in Germany. The data collection that underpins these systems has also been found to be unlawful, as in France.

Inaccuracy

In many cases, these systems are fundamentally inaccurate. They produce serious inaccuracies or false positives, potentially implicating innocent people. In many cases, the police, law enforcement or criminal legal system authorities have not meaningfully or properly evaluated their accuracy before deploying them. Even when such tests have been conducted, they have sometimes continued to use systems with poor rates of accuracy.

Accuracy, however, is not a panacea. An 'accurate' system would merely serve to uphold and reproduce the discrimination inherent in the data it was using.

Prohibition

As demonstrated in this report, the location-focused and individual-focused 'predictive', profiling and 'risk' assessment systems in this report lead to racial and socio-economic profiling, discrimination and criminalisation.

Their use leads to unjust and discriminatory consequences, from surveillance to stop and search, from police harassment and violence to arrest, from detention

to deportation.

The conclusion of this report, and those that underpin it, is the same: these systems must be prohibited.

National legislatures where these systems are being used should pass a legal prohibition against their use. Similarly, local legislatures or councils where these systems are being used, such as a city or local council, should also seek to pass a prohibition within their jurisdiction.[209]

There are current and long-standing campaigns against the use of these systems in Europe and elsewhere, such as the campaign to ban predictive policing systems in the EU AI Act,[210] the ***Technopolice*** campaigns in France[211] and Belgium,[212] the ***Safety Not Surveillance*** coalition in the UK[213], and ***Stop LAPD Spying*** in the US.[214] Supporting these campaigns, and others like them, is vital as governments, police forces, criminal legal authorities and companies seek to extend the use of algorithmic, automated and artificial intelligence systems.

MENSONGES - RACISME - ETOUFFEMENT - SEXISME - ARME DE GUERRE - PERMIS DE TUER
STOP À L'IMPUNITÉ POLICIÈRE
#PAS DE JUSTICE PAS DE PAIX
STOP AU DÉNI DE JU

> “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.

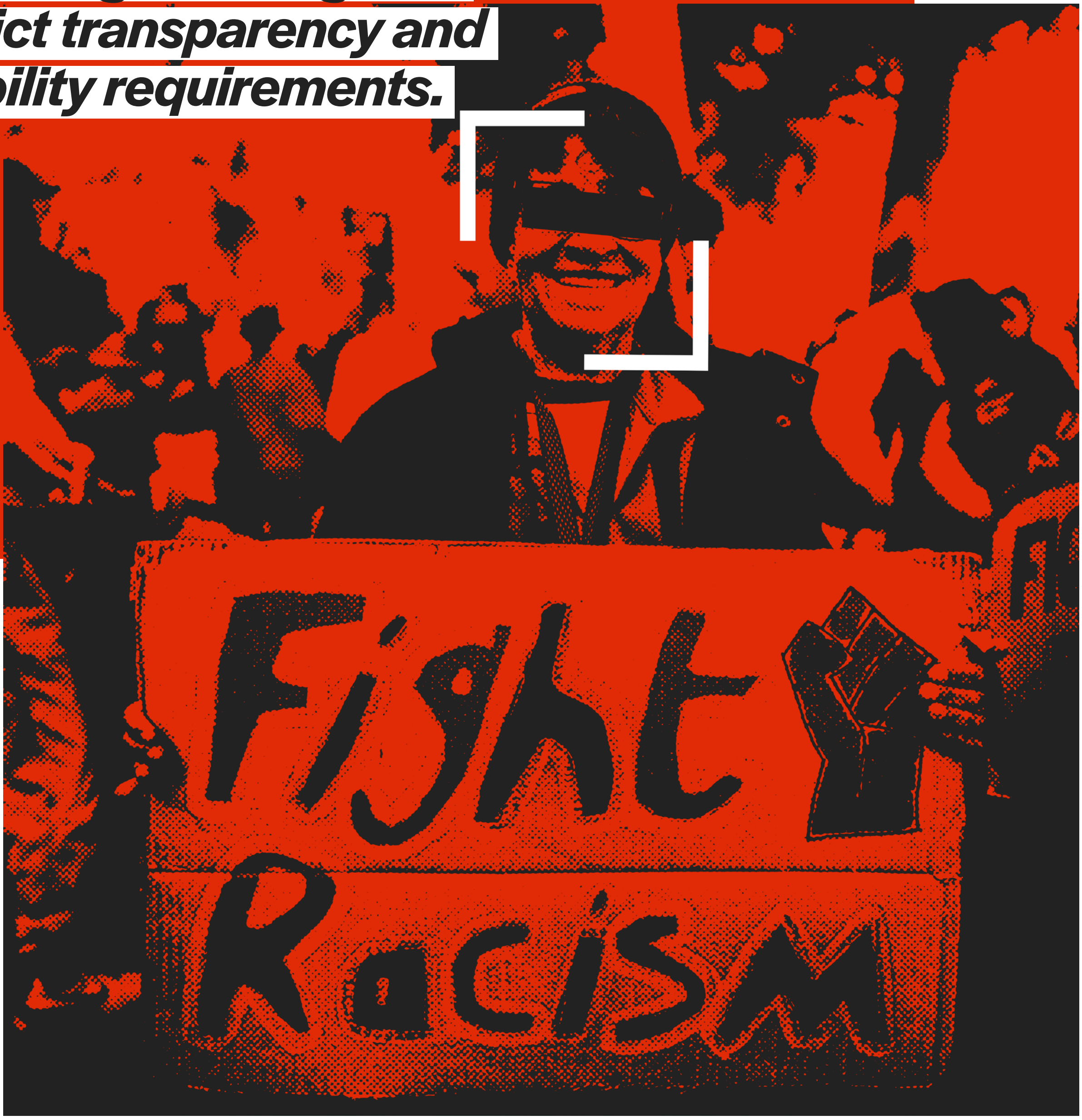


Image credits

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: “manif 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: “manif 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: “manif 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: “manif contre la «Loi Sécurité globale» à Paris le 28 novembre 2020 (4)” Jeanne Menjoulet

Page 63: “Fight Racism !” by Alisdare Hickson

Endnotes

[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)

[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

[3] Cabinet Office et al, ‘Ethics, Transparency and Accountability Framework for Automated Decision-Making’, 2021

[4] Cambridge Dictionary, ‘Machine learning’

[5] Amnesty International, ‘We Sense Trouble: automated discrimination and mass surveillance in predictive policing in the Netherlands’, 2020

[6] Lawrence Sherman, ‘The Cost-Effectiveness of Evidence-Based Policing’, 2010

[7] 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

[8] EDRi, ‘Civil society calls on the EU to ban predictive AI systems in policing and criminal justice in the AI Act’, 2022

[9] European Union Agency for Fundamental Rights, ‘Second European Union Minorities and Discrimination Survey - Main results’, 2017, page 26, 29

[10] European Union Agency for Fundamental Rights, ‘Being Black in the EU — Experiences of people of African descent’, 2023

[11] France 24, ‘Police violence: How can France tackle racial profiling without first addressing race?’, 9 July 2023,

[12] Amnesty International, ‘YOU NEVER KNOW WITH PEOPLE LIKE YOU’ POLICE POLICIES TO PREVENT ETHNIC PROFILING IN BELGIUM’, May 2018

[13] Rights International Spain and Open Society Justice Initiative, ‘Under Suspicion: The Impact of Discriminatory Policing in Spain’, 2019; Video version

[14] Arenas-García L and García-España E, ‘Police stop and search in Spain: an overview of its use, impacts and challenges’, March 2022.

[15] Bundeszentrale für Politische Bildung, ‘Migration und Kriminalität – Erfahrungen und neuere Entwicklungen‘, 25 September 2020

[16] 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

[17] Fair Trials, ‘Disparities and Discrimination in the European Union’s Criminal Legal Systems’, 2021

[18] 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.

[19] 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

[20] Germany report

[21] Palantir, ‘Palantir reports Q4 2024 Revenue Growth’, 2025,

[22] 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.

[23] Find more information on the company’s involvement in the Israeli occupation of Palestine on the Database of Israeli

Military and Security Export webpage.

24 Find more information on the use of ClearView software by US police

25 El Salto (2021), 'El Estado policial español 2.0: tecnologías de empresas privadas para vigilar a los ciudadanos'. 4 February 2021

26 Find more information on SopraSteria's contract with the EU for the 'Shared Biometric Matching System' (sBMS)

27 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

28 Forbes, 'Meet The Ex-NSA And Ex-Unit 8200 Spies Cashing In On Security Fears', 10 September 2014

29 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. According to this definition, this report covers only predictive analytics for crime 'prediction', and AI video surveillance.

30 Ibid.

31 Article 5, 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),

32 Chapter II, Article 5(d), 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

33 EU Commission, 'Commission publishes the Guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act', 4 February 2025

34 Fair Trials, 'EU Parliament approves landmark AI law', 16 June 2023,

35 Investigate Europe 'France spearheads member state campaign to dilute European AI regulation', 22 January 2025; TIME, 'Big Tech Is Already Lobbying to Water Down Europe's AI Rules', 21 April 2023,

36 European Digital Rights (EDRi), Access Now, Algorithm Watch, Bits of Freedom, European Disability Forum (EDF), European Not for Profit Law Center, Fair Trials, Panoptykon Foundation, and PICUM, 'Artificial Intelligence Act Amendments - Ensure meaningful transparency of AI systems for affected people', November 2021,

37 Article 86, AI Act

38 Article 50, AI Act

39 European Digital Rights (EDRi), Access Now, Algorithm Watch, Bits of Freedom, European Disability Forum (EDF), European Not for Profit Law Center, Fair Trials, Panoptykon Foundation, and PICUM 'Artificial Intelligence Act Amendments - Ensure rights and redress for people impacted by AI systems', November 2021

40 Article 85, AI Act

41 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.

42 Spain report

43 Germany report

[44] Braga, Anthony A., Barao, Lisa, ‘Targeted Policing for Crime Reduction’, Handbook on Crime and Deviance, Handbooks of Sociology and Social Research, Springer, 2019

[45] EU Commission, ‘Commission publishes the Guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act’, 4 February 2025

[46] Germany report

[47] Knobloch, Tobias, ‘Vor die Lage kommen: Predictive Policing in Deutschland’, Stiftung Neue Verantwortung, 29 August 2018

[48] Germany report

[49] Germany report

[50] Camacho-Collados, M., & Liberatore, F, ‘A decision support system for predictive police patrolling’. *Decision support systems,75*, 25-37, 2015

[51] El Salto, ‘El Estado policial español 2.0: tecnologías de empresas privadas para vigilar a los ciudadanos’, 4 February 2021

[52] France report

[53] Belgium report

[54] Orbit GIS. *Zones de police*. URL: www.orbitgis.com/fr/zone-de-police

[55] *The Markup*, ‘Crime Prediction Software Promised to Be Free of Biases. New Data Shows It Perpetuates Them’, 2021

[56] Florian Gauthier, ‘Prédire les vols de voitures ?’, *Etalab blog,* 2018

[57] Abgeordnetenhaus Berlin, ‘Bericht des Senats gemäß § 21 Absatz 4 Allgemeines Sicherheits- und Ordnungsgesetz (ASOG) für das Jahr 2021’, 22 July 2022

[58] France report

[59] Germany report

[60] Germany report, Interview with Egbert, Simon, Postdoctoral Researcher ‘The Future of Prediction’, University of Bielefeld, 04 October 2023

[61] Haco. ‘Politiezone Westkust experimenteert met datasets in strijd tegen criminaliteit’, *De Standaard*. 17 May 2016

[62] El Salto, ‘El Estado policial español 2.0: tecnologías de empresas privadas para vigilar a los ciudadanos’, 4 February 2021

[63] Polizei Berlin, ‘Kriminalitätsbelastete Orte’

[64] Orbit gis.Zones de pólice; Orbit gis.Zones de police – Stratégie

[65] Haco. ‘Politiezone Westkust experimenteert met datasets in strijd tegen criminaliteit’. *De Standaard*. 17 May 2016

[66] France report

[67] Europcop, ‘Analysis and prediction of crime’

[68] Minister of Interior’s answer of 09/07/2020 to written question n°7-591. *Belgian Senate*,

[69] France report

[70] France report

[71] 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; 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

[72] Ibid

[73] Article 10, Law Enforcement Directive

[74] Recital 38 and Article 11, Law Enforcement Directive

[75] German report, France report, Belgium report.

76 Polizei Berlin, 'Kriminalitätsbelastete Orte')

77 France report

78 Lina Schmid, 'Grundrechte in Gefahr(engebieten). Verfassungsrechtliche Beurteilung der polizeilichen Praxis "kriminilatitätsbelasteter Orte", 2023, in *Mythos Generalverdacht. Wie mit dem Mythos Clankriminalität Politik gemacht wird,* Nautilus Flugschrift, p.167, translated from German.

79 Süddeutsche Zeitung, 'Unbeteiligte geraten ins Kontrollraster', 12 Sept 2014

80 Lina Schmid, 'Grundrechte in Gefahr(engebieten). Verfassungsrechtliche Beurteilung der polizeilichen Praxis "kriminilatitätsbelasteter Orte", 2023, in *Mythos Generalverdacht. Wie mit dem Mythos Clankriminalität Politik gemacht wird,* Nautilus Flugschrift, p.167.

81 Wrangelkiez United, 'Perspektiven: Realitäten von Geflüchteten', Video.

82 Ibid

83 George L. Kelling and James Q. Wilson, *The Atlantic* , 'Broken Windows: The Police and Neighbourhood Safety', 1982

84 Donna Ladd, 'Inside William Bratton's NYPD: broken windows policing is here to stay', *The Guardian,* 2015

85 'Northeastern University researchers find little evidence for 'broken windows theory,' say neighborhood disorder doesn't cause crime', *Northeastern Global News*, 15 May 2019

86 Amnesty International UK, 'Automated Racism: How police data and algorithms code discrimination into policing', February 2025

87 Risk Terrain Modelling, 'Spatial dynamics of crime'

88 Ibid.

89 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).

90 Camille Gosselin, 'La police prédictive : enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique', Paris: IAU Île-de-France, 2019

91 Belgium report

92 Sûreté Globale

93 France report

94 Risk Terrain Modelling, 'Spatial dynamics of crime'

95 Thibault Sardier, 'Cartographie criminelle : surveiller et prédire', lemonde.fr, 5 January 2018

96 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

97 International terrorism database. It shows that France only has 20 entries from 2016 to 2019, which leaves one wondering about the relevance of this dataset.

98 France report

99 France report

100 Amnesty International UK, 'Automated Racism: How police data and algorithms code discrimination into policing', February 2025

101 Amnesty International UK, 'Automated Racism: How police data and algorithms code discrimination into policing', February 2025, p.69

102 Ibid

103 Ibid.

104 Fair Trials, 'Automating Injustice: The Use of Artificial Intelligence &

Automated Decision-Making Systems in Criminal Justice in Europe', 09 September 2021

105 Gatti, Carlo, 'Monitoring the monitors: a demystifying gaze at algorithmic prophecies in policing', 10 November 2022, *Justice, Power and Resistance*, *5*(3), 227-248

106 AlgorithmWatch, 'The Rise and Fall of a Predictive Policing Pioneer', 7 November 2024; Wired, 'Perché la più avanzata startup italiana di polizia predittiva è sull'orlo del baratro', 31 January 2024

107 Gatti, Carlo, 'Monitoring the monitors: a demystifying gaze at algorithmic prophecies in policing', 10 November 2022, *Justice, Power and Resistance*, *5*(3), 227-24

108 *Ibid.*

109 AlgorithmWatch, 'Automating Society Report 2020 — Swiss Edition', January 2021

110 Belgium report

111 Williams, P, 'Criminalising the Other: challenging the race-gang nexus', *Race & Class*, 2014, *6*(3), 18-35

112 Belgium report

113 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

114 Belgium report

115 'EU: Definition of "potential terrorists" opens door to broad information-sharing', *Statewatch*, 2 October 2024

116 Bundeskriminalamt, 'RADAR (Regelbasierte Analyse potentiell destruktiver Täter zur Einschätzung des akuten Risikos)',

117 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),

118 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; Nature, 'Police use a computer to expose false testimony', 30 May 2018

119 Civio, 'Spanish National Police stop using Veripol, its star AI for detecting false reports', 25 March 2025

120 Germany report; 'PNR for all: UN Security Council mandates worldwide air travel surveillance and profiling, biometric collection, terrorist watchlists', *Statewatch*, 8 January 2018

121 Germany report.

122 Tony Bunyan, 'EU: The surveillance of travel where everyone is a suspect', *Statewatch*, August 2008

123 European Commission, ''ProtectEU: a European Internal Security Strategy', COM(2025) 148 final, 1 April 2025

124 Senate, **'Orden de servicio 3/2018'**, February 2018

125 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; AlgorithmWatch (2021), 'In Catalonia, the RisCanvi algorithm helps decide whether inmates are paroled', 25 May 2021

126 Justizportal Nordrhein-Westfalen, § 25a HSOG Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) Landesrecht Hessen; Gesellschaft für Freiheitsrechte, 'NRW Assembly Act:

Threat to freedom of assembly and civilsociety'

127 Germany report

128 Harry Davies, Bethan McKernan, Dan Sabbagh. 'The Gospel': how Israel uses AI to select bombing targets in Gaza', *The Guardian,* 1 December 2023

129 Rights International Spain and Open Society Justice Initiative, 'Under Suspicion: The Impact of Discriminatory Policing in Spain', 2019. Report, Video; Arenas-García L and García-España E, 'Police stop and search in Spain: an overview of its use, impacts and challenges', March 2022

130 Bundeszentrale für Politische Bildung, 'Migration und Kriminalität – Erfahrungen und neuere Entwicklungen', 25 September 2020

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

132 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,

133 Germany report

134 Welt, 'So funktioniert das Radar für radikale Islamisten', 12 June 2017

135 Germany report

136 Germany report

137 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

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

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

140 Tagesschau, 'Immer mehr rechte Gefährder', 26 June 2022

141 Belgium report

142 Germany report

143 Germany report

144 Germany report

145 Secretary of State for Security, 'Instruction nº 7/2016', 8 July 2016

146 Bayona, J. Z, Violencia contra la mujer: marco histórico evolutivo y predicción del nivel de riesgo (Doctoral dissertation, Universidad Autónoma de Madrid), 2014

147 Kanzlei Redecker Sellner Dahs, 'Stellungnahme an das Verwaltungsgericht Wiesbaden', 09 September 2021

148 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

149 *Ibid*

150 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

151 Ministry of Interior, 'Statistical data Viogen', September 2023

152 Germany report

153 Germany report

154 Germany report

155 MDR, 'Sachsen-Anhalt will Polizei-Gewahrsam bei Terrorverdacht verlängern', 17 December 2023

156 Ibid

157 Tagesspiegel, 'Neue Plätze für 40 Straftäter – im Abschiebeknast', 31 January 2024

158 Tagesschau, 'Warum die Abschiebepläne kaum einzuhalten sind', 04 October 2022

159 Deutscher Bundestag, 'Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE, Drucksache 19/5202, Personenpotentiale islamistischer „Gefährder"', 9 November 2018 (translated from German)

160 Amnesty International UK, 'Automated Racism: How police data and algorithms code discrimination into policing', February 2025

161 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; Statewatch OASys news piece forthcoming

162 Fair Trials, 'Automating Injustice: The Use of Artificial Intelligence & Automated Decision-Making Systems in Criminal Justice in Europe', 09 September 2021.

163 *Ibid.*

164 Fair Trials, 'My sons were profiled by a racist predictive policing system – the AI Act must prohibit these systems', 28 September 2022

165 Fair Trials, 'Automating Injustice: The Use of Artificial Intelligence & Automated Decision-Making Systems in Criminal Justice in Europe', 9 September 2021; Gatti, Carlo, 'Monitoring the monitors: a demystifying gaze at algorithmic prophecies in policing', 10 November 2022, *Justice, Power and Resistance*, *5*(3), 227-248.

166 La Quadrature du Net, 'Non à la vidéosurveillance algorithmique, refusons l'article 7 de la loi olympique!', 18 January 2023

167 'Law Enforcement and Corrections' webpage on the ISS website

168 El Pais, 'Marbella, el mayor laboratorio de videovigilancia de España', 22 November 2019

169 La VanGuardia, 'Madrid has 83 cameras on the streets with artificial intelligence Surveillance', 9 January 2025

170 Nicolas Bocquet, 'The Brussels Smart City: how "intelligence" can be synonymous with video surveillance'. *Brussels Studies*, 2021

171 La Quadrature du Net, 'France becomes the first European country to legalize biometric surveillance' 29 March 2023

172 Jacobin, 'Emmanuel Macron Is Using the 2024 Olympics to Make France a Surveillance State', 21 March 2023

173 Jacobin, 'France Wants to Make Olympics-Style Surveillance Permanent', 23 October 2024

174 ID Tech Editorial Team, 'French Court Rules Briefcam's AI Surveillance System Unlawful', 31 January 2025

175 Ibid.

176 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

177 Ibid.

178 Germany report

179 Niedersächsischer Landtag, 'Antrag, Einsatz künstlicher Intelligenz zur Suizidprävention und Verbesserung der Sicherheit in niedersächsischen Justizvollzugsanstalten', Drucksache 18/8729, 09 March 2021

180 Landesbeauftragte für den Datenschutz Niedersachsen, '27. Tätigkeitsbericht 2021', 2021

181 Germany report

182 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

183 Rhue, Lauren, 'Racial Influence on Automated Perceptions of Emotions', 9 November 2018

[184] Article 19, ‘Emotional Entanglement: China’s emotion recognition market and its implications for human rights’, 19 November 2020.

[185] Germany report

[186] AlgorithmWatch, ‘Spanish Inmates Not to Be Automatically Monitored in Fear of AI Act’, 28 March 2024

[187] Belgium report

[188] Statewatch, ‘France: Green light for police surveillance of political opinions, trade union membership and religious beliefs’, 13 January 2021

[189] France report

[190] France report

[191] Camille Gosselin, ‘La police prédictive : enjeux soulevés par l’usage des algorithmes prédictifs en matière de sécurité publique’, (Paris: IAU Île-de-France, 2019)

[192] Ibid

[193] 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

[194] La Quadrature du Net, ‘La reconnaissance faciale des manifestantes est déjà autorisée’, 18 November 2019.

[195] France report

[196] 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

[197] France report

[198] Sainz de la Maza Quintanal, E, ‘“Ultima ratio”: el proceso de expulsión de inmigrantes en situación irregular en España’, 2015

[199] 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

[200] Belgium report, Germany report, France report

[201] Matthias Monroy, ‘Suspicion files: German police databases on political activists’, *Statewatch*¸ 10 April 2018

[202] Belgium report

[203] Belgium report

[204] Belgium report

[205] Rights International Spain and Open Society Justice Initiative, ‘Under Suspicion: The Impact of Discriminatory Policing in Spain’, 2019. Report; Video

[206] Belgium report, France report

[207] Belgium report

[208] Belgium report, France report

[209] Reuters, ‘In a U.S. first, California city set to ban predictive policing’, 19 June 2020

[210] EDRi, ‘Civil society calls on the EU to ban predictive AI systems in policing and criminal justice in the AI Act’, 1 March 2022

[211] https://technopolice.fr/

[212] https://technopolice.be/

[213] https://www.openrightsgroup.org/campaign/safety-not-surveillance/

[214] https://stoplapdspying.org/