AUTOMATED DISCRIMINATION

'Predictive' Policing and Data-Profiling in Belgium

Front page photo:
Antwerp Police Force Headquarters

AUTOMATED DISCRIMINATION

'Predictive' Policing and Data-Profiling in Belgium

April 2025


STATEWATCH


LIGUE
DES DROITS
HUMAINS


LIGA
VOOR
MENSEN
RECHTEN


European
Artificial Intelligence
& Society Fund


TECHNOPOLICE.BE


tac
tiC

Methodology

Main author: Corentin Debailleul.

Supervision, editing and proof reading by Griff Ferris and Sofia Lyall.

Desk research by Griff Ferris, Sofia Lyall, Nathalie Vandevelde, Maria Karantoumani, and Corentin Debailleul.

Questions on the use of specific databases were sent to a series of local police forces identified as strategic targets.

Freedom of information (FOI) requests were sent by the Lig*ue des droits humains* (LDH) commission on privacy and ICT to all French-speaking local police forces and municipalities, and to the largest Flemish cities (Ghent and Antwerp), regarding surveillance devices and their location; related public procurement documents; and related Data Protection Impact Assessments (DPIA'S). FOI'S were also sent to the Federal Police, regarding i-Police and face recognition surveillance.

Information was **triangulated** by checking available information in the press; on public procurement websites; in the minutes of parliamentary debates and police and municipal councils.

Interviews carried out by Griff Ferris and Sofia Lyall:

Date	Name and/or position
2023-02-17	Frank Schuermans, Supervisory Body for Police Information (COC) Acting Chairman
2023-04-04	Catherine Forget, Lawyer and university researcher, specialised in police databases

Interviews carried out by Corentin Debailleul:

Date	Name and/or position
2023-06-16	Chief Commissioner at the judicial Federal Police, Senior advisor for Research & Development and ict strategy to the General Director of the Federal Judicial Police
2023-06-28	Gregory Lewkowicz, ULB law professor involved in a research program to develop an AIsystem
2023-07-03	Data protection officer (DPO) of a local police force
2023-08-04	Coordinator of a non-profit supporting male and trans sex workers (Brussels)
2023-08-08	Nina Henkens & Onur Cevik, Social workers from Kif Kif (Antwerp)
2023-08-17	Union delegates, Federal Police
2023-09-19	A legal expert, formerly working at the Federal Police

2023-09-28	Farah Kassem, KU Leuven researcher on (de)radicalisation
2023-10-11	Frank Schuermans, Supervisory Body for Police Information (COC) Acting Chairman

Finally, informal discussions were held with members of the LDH commission on privacy and ICT; members of the Brussels technopolice collective; a social worker from Antwerp working with trans sex workers; a policy advisor from the Belgian Union of sex workers UTSOPI; a source within the Federal Police; and a lawyer, member of the *Observatoire international des prisons – section belge.*

Special thanks to Emmanuelle de Buisseret Hardy, Manuel Lambert, Rémy Farge, Fien De Meyer, Chris Jones, and Sarah De Laet.

Contact: corentin.debailleul@ulb.be

Layout by Margaux Hallot.

Executive summary

Police in Belgium, as elsewhere in the world, are increasingly using advanced data analysis techniques to try to 'predict' crime. The supposed benefits of this are increased police 'efficiency' and 'effectiveness' through the mastery of algorithms, data, and 'innovation'.

However, this new digital era of crime control is beset by problems. Police data is often inaccurate and reflects systemic biases within the police and wider society – in particular racism, Islamophobia and classism. The laws, procedures and systems in place do not properly control how it is gathered, stored, shared and used. Those affected have few opportunities for redress, and the opportunities that do exist are often so flawed as to be ineffective.

This report highlights these serious problems through an analysis of three broad topics:

- Location-focussed 'predictive' policing systems used by local Belgian police forces;
- the databases that are or will be used to inform those systems; and
- the Belgian Federal Police 'i-Police' project, designed to use data from police and other public agencies, as well as a range of other data sources, to inform police decision-making and activities.

Predictive policing

'Predictive' policing and data profiling techniques rely on data analysis and algorithms to supposedly 'predict' and then seek to 'prevent' potential criminal activity. The alleged aims are:

- to allow the more efficient allocation of police resources;
- to 'predict' or profile individuals and locations as criminal;
- to justify police interventions such as surveillance and monitoring, questioning, stop and search or even arrest.

Local Belgian police forces

A variety of tools and systems are used by local Belgian police forces for these purposes. The Geographical Information System produced by the company Columba is particularly notable. It takes geographic data from historic crime reports to identify supposed crime 'hotspots'. The company claims it is used by almost 100 police forces in Belgium. Other tools offered by the company are designed for "crime analysis" and public order policing (for example, of protests).

The Westkust police force covers the Flemish municipalities of La Panne, Koksijde and Nieuwpoort, and was a forerunner of the Flemish police's digitisation process. A visit by the local police chief to the United States inspired a plan to use police data to "roughly predict where things could potentially go wrong," in the words of the chief. The location-focussed system has allegedly led to a 40% reduction in criminal incidents, but there has been no objective evaluation of the system or its functioning.

The Zennevallei police force covers the municipalities of Beersel, Halle and Sint-Pieters-Leeuw in the Flemish south-west suburbs of Brussels. Its interest in 'predictive' policing led to a project with Ghent University, designed to 'predict' burglaries. This used both historical crime information and other data, such as weather conditions.

The system is based on a method known as Risk Terrain Modelling, which is used to try to identify areas likely to be at higher risk of crime because of so-called 'environmental factors' and spatial attributes. The criminological theories that underpin this approach have been widely-criticised for failing to take into account the multiple, complex, and structural causes of crime. The researchers behind the project have called for the use of even more data to improve the functioning of the system, and they have EU financial backing to do so.

Police in the major port city of Antwerp, and across the country, have acquired body-worn cameras through a deal between Antwerp and the Swedish corporation Securitas. The company has also taken over certain activities from the Antwerp police, such as monitoring CCTV footage.

Separately, the police in Antwerp have developed their own smartphone application, called FOCUS. This gives police officers in the street access to federal databases along with multiple other functions, such as reporting and messaging services. Alongside this, the police force aggregates data from multiple sources into a single platform: ANPR systems, police car locations, CCTV cameras and crowd management via mobile phone tracking. They have also applied advanced analytics techniques, including text recognition, human parsing, behavioural profiling and object tracking, to CCTV images.

These systems, tools and techniques raise a number of issues for the protection of civil liberties and human rights. Location-focussed 'hotspot' policing has been shown in multiple contexts to perpetuate discriminatory patterns and excessive policing of particular individuals or areas. The theories that underpin it are narrow and discredited. The integration of a growing number of data sources compounds these problems, raising further issues regarding privacy, data minimisation and risk of misuse or leaks.

'Predictive' systems such as those used by local police forces in Belgium infringe upon core principles of justice, including the right to liberty, the right to a fair trial, and the presumption of innocence. Individuals, groups, and locations are prematurely labelled as potential threats. This can lead to pre-emptive punitive

measures, such as unjustified deprivations of liberty. This erodes the essential principle that individuals are considered innocent until proven guilty, and poses a severe risk of miscarriages of justice.

Police databases

Much of the data used in these systems comes from police databases. These pose a fundamental problem for 'predictive' policing tools. A vast number of police databases are in use in Belgium, yet there is little effective control or oversight over their structure or use. Laws on data protection are enforced poorly, if at all. Officers who illegally access or use data face few meaningful sanctions, if any.

This lack of control and supervision is all the more striking given the number of police databases in Belgium, and the huge array of data they may contain. Official police and criminal justice data is structured according to the systemic biases of the police and of the society in which they operate. It is also often inaccurate.

Unofficial data may be no more than hearsay, gossip, rumour, speculation, or simply invented – as in the case of a man whose entry on the database claimed he planned to infect police officers with HIV. On the other hand, data collection schemes may also serve to further marginalise people in already-difficult situations. That problem is demonstrated in this report by the example of an app shared between the Antwerp administration and police for registering sex workers. Supposedly for the purpose of guaranteeing their safety, the database meant that sex workers in precarious immigration situations were driven further from support services and organisations, as registering in the app could eventually lead to deportation.

Police databases are also accessed for a growing range of purposes. Few people would be surprised that they are used to vet prospective employees for example who may be granted access to classified information or to sensitive areas such as nuclear sites. Their use to vet people applying to work at music festivals may however raise eyebrows.

This report recounts the experience of a young man barred from the employment he was seeking because he was wrongfully accused of participating in a protest. That accusation (and arrest) still leads to him being stopped and questioned at airports. Independent reports have also recounted a disproportionate number of security clearances being denied to workers of North African origin.

The effects of these prejudicial policies have been extensive and varied. Individuals have encountered financial losses and difficulties in securing employment due to the refusal of financial services. This financial hardship further exacerbates their susceptibility to harm and marginalisation. Moreover, Belgian law does not offer a meaningful right for people to access their data, making it extremely difficult – if not impossible – to rectify or delete inaccuracies.

The i-Police system

The i-Police system has been in the works for at least a decade. It is currently in the hands of the federal police and the corporation Sopra Steria, with support from the international consultancy firm KPMG and an array of subcontractors. Amongst those subcontractors are a number of Israeli companies, including companies whose founders or CEO's are former Israeli military intelligence officials. This raises serious questions over the ethical commitments of the Belgian authorities, as well as the possibility of potential 'back doors' that would allow illegal access to data.

An official announcement has said the system:

> "automatically analyses and cross-checks data such as camera images, photos, fingerprints, traces and documents. These features enable criminals and criminal phenomena to be identified more quickly and more clearly. Investigators receive a wealth of information filtered in real time, enabling them to take rapid, targeted action".

A number of location-focused 'predictive' functions for the system have been planned. The ability for officers to receive real-time updates on individuals of interest – for example, when that individual is encountered by another officer – has also been touted.

As with the local police force systems examined in this report, these plans – however far-fetched they may seem – rely on the integration and analysis of vast amounts of data. This is supposed to come from both international and national government agencies, private companies, and publicly-available sources such as social media or the press. These sources contain both verified and unverified information. Along with issues of proportionality and necessity, the problem of hearsay, rumour, or a flawed algorithm informing police actions once again raises its head. Automating the analysis of video surveillance footage for 'suspicious' activity raise similar issues, alongside questions of the basic desirability of these technologies for a supposedly democratic society.

As with many government IT projects, however, the future is less certain than it seemed when the i-Police project was first announced. There are ongoing campaigns against the use of Israeli technologies and subcontractors by the Belgian police, supervisory bodies are deeply concerned about the inappropriate collection and use of data, and the Belgian Federal police are running out of money. Any one of these factors should be enough to call into question the necessity of such a project. The three of them combined should, one would hope, be enough to put an end to it once and for all. Whether that is so remains to be seen.

Prohibition now

First and foremost, 'predictive' AI systems are known to disproportionately target and discriminate against marginalised groups and reinforce existing structural inequalities. Data inputs drawing on race, religion, socio-economic status, migration status, and nationality often become determining factors in the unfair over-policing, surveillance, and criminalisation of certain communities. They impinge upon, undermine and violate multiple rights: to liberty, to a fair trial, to freedom from discrimination, to the presumption of innocence, and so on.

A lack of transparency and accountability, and no access to effective remedies, compounds these issues. 'Predictive' AIsystems operate behind technological and commercial barriers, shielding decisions from scrutiny. Affected individuals are left in the dark, with no clear and effective means to open the 'black boxes' and challenge these opaque decisions.

Belgian law offers few meaningful protections against, or means of redress for, these deep-rooted problems. The EU's recent Artificial Intelligence Act is unlikely to help much in this regard – and it is in any case clear that the Belgian authorities have failed to correctly implement existing EU law purportedly designed to protect individuals, such as data protection rules.

Legal protections that already exist must be enforced, and new legal mechanisms must be introduced to complement them. However, to fully account for the harms arising from data-driven policing in Belgium, such regulatory proposals do not go far enough. This report has highlighted structural issues of racism, Islamophobia and classism in policing. These issues are systemic and cannot be resolved through regulation of police algorithms or data usage alone.

In light of these pressing concerns, it is imperative that Belgium prohibits the use of 'predictive' policing and automated decision-making systems in policing and criminal justice settings. By banning these systems, Belgium can take a significant step towards building a more equitable, just, and democratic society. It is an opportunity to reaffirm the commitment to upholding fundamental rights, promoting equality, and maintaining the principles of justice and accountability.

"Policing in the 21st century will be digital – or it won't be"
Annelies Verlinden, Belgian Minister of Interior (2020-2025)*

* Annelies Verlinden. 2023. 'Projet de police d'avenir, pour une Belgique plus sûre'. In: *Etats généraux de la police: Un plan pour la police du futur*. Brugge/Genval: Vanden Broele. p. 699.

Acronyms and abbreviations

ADM	Automatic or algorithmic decision making
AI	Artificial intelligence
ANPR	Automatic number plate recognition
BNG-ANG	*Banque nationale générale – Algemene nationale gegevensbank* (National General Database)
CERD	United Nations Committee on the Elimination of Racial Discrimination
COC	*Controleorgaan op de politionele informatie – Organe de contrôle de l'information policière* (Supervisory Body for Police Information)
CPPL-VLCP	*Commission Permanente de la Police Locale – Vaste Commissie van de Lokale Politie* (Permanent Committee of the Local Police)
DIV	*Direction pour l'immatriculation des véhicules – Dienst voor inschrijvingen van voertuigen* (Vehicle registration service)
DPA	Data protection authority
DPIA	Data protection impact assessment
DPO	Data protection officer
DRI	Directorate of Police Information and ICT Resources
ECJ	European Court of Justice
FEEDIS	Feeding information system (used by the Federal Police)
FRT	Facial recognition technology
GAFAM	Google, Apple, Facebook, Amazon, Microsoft
GDPR	General Data Protection Regulation
GPI	*Geïntegreerde politie – Police intégrée* (Integrated Police)
ILP	Intelligence-led policing
ISLP	Integrated system for local police
LDH	*Ligue des droits humains* (Belgian French-speaking Human Rights League)
LEZ	Low Emission Zone
NACE	*Nomenclature statistique des activités économiques dans la Communauté européenne* (Statistical Classification of Economic Activities in the European Community)
OSINT	Open-source intelligence
QLP	Quantitative Legal Prediction
SICAD	*Service d'information et de communication de l'arrondissement* (District information and communication service)
ULB	*Université libre de Bruxelles*
VCA	Video content analysis
VUB	*Vrije Universiteit Brussel*

Back cover page photo:
Charleroi Police Force Headquarters
La Tour Bleue, designed by Jean Nouvel