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

Table of content

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)[1]

1 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.

Introduction

In recent years, police forces around the world have significantly increased their use of data analysis and data profiling. They have introduced 'predictive' policing and crime 'prediction' systems into their operations, presenting these as transformative methods that could reshape the landscape of crime prevention and investigation. The so-called 'police science' approach claims to amplify policing's supposed 'efficiency' and 'effectiveness' through the mastery of algorithms, data, and 'innovation'. This apparently marks the beginning of a new digital era for crime control.

'Predictive' policing and data profiling are law enforcement approaches that rely on data analysis and machine learning algorithms to supposedly 'predict' and then seek to 'prevent' potential criminal activity. They use historical crime data, along with various other socio-demographic and environmental factors, to identify patterns and trends that suggest where and when a crime is most likely to occur, or by whom it may be committed.

The primary aims of 'predictive' policing and data profiling are:

- to allocate police resources more efficiently by anticipating and pre-empting criminal activity in certain locations or areas;
- to 'predict' or profile individuals as (potential) criminals to monitor them more closely;
- to justify police interventions such as questioning, stop and search or even arrest.

However, data profiling and 'predictive' policing raises concerns about data bias, discrimination, potential breaches of human rights and civil liberties. The systems' reliability can be questioned, especially as the theories underpinning them are questionable. The approach also carries the risk of self-fulfilling prophecies. Increased police presence in certain areas is likely to lead to policing and criminal justice outcomes such as stop and search and potentially arrests. These outcomes are then represented in data fed into the systems. This results in police further repeatedly targeting the same areas, creating a feedback loop.

Similarly, data-driven policing may lead to the targeting of people from a certain background or who fit a certain profile, often racialised or marginalised people. They may then face policing or criminal justice outcomes such as stop and search and arrest. When fed back into police data it will result in a similar feedback loop of police repeatedly targeting people who fit that profile.

There are also transparency issues. Algorithms can be opaque and incomprehensible, yet accountability is crucial for people to be able to challenge these systems and their outputs. Ultimately, fundamental human rights can be endangered, including the presumption of innocence; the right to privacy, to liberty and to a fair trial; the freedom of assembly and association; and equal treatment before the law.[2]

2 Thomas Marquenie. 2022. 'Het gebruik van AI-toepassingen binnen het politiewezen: voordelen, risico's en best practices'. Staten Generaal over Artificiële Intelligentie. *Centre for IT & IP Law (CiTiP)*. 17 June 2022.

‘Predictive’ policing in Belgium constitutes a complex tapestry of evolving initiatives across federal and local law enforcement agencies. This report uncovers the multi-layered dimensions of data-based and ‘predictive’ policing in Belgium. It examines the underlying technologies, theories, and societal implications.

The report analyses a large body of information, including press reports, public communications, official documents, and parliamentary questions and debates. In addition, it utilises reports from government agencies and non-governmental organisations, as well as a private audit of the IT department of the Federal Police. It also draws on academic literature regarding ‘predictive’ policing systems in Belgium.

The report also draws on interviews conducted with police officials and representatives of associations involved in human rights or with groups that may be subject to police monitoring, such as racialised groups and sex workers. Freedom of information (FOI) requests were filed, but the police used security exceptions to limit the information provided to that which was already publicly-available.

The report is divided into four sections. The first covers the predictive capabilities of the police and covers initiatives taken by local police forces. The second looks at Belgian police databases, which provide much of the data for predictive systems, and describes the different risks associated with their use. The third section looks at the Federal Police’s i-Police programme and its many ramifications. Finally, the fourth and last section describes the few rudiments of predictive justice being developed in Belgium. The report concludes with a reflective summary of our study.

This report aims to go beyond simply observing technology in action. In an age where data and algorithms dominate decision-making, our goal is to expose the challenges and hazards posed by this transformation. The direction of ‘predictive’ policing is not predetermined. It is influenced by the actions and choices made by individuals, communities, policymakers, and advocates. It is the joint responsibility of all of us to guarantee that the way forward signifies justice, fairness, and the steadfast protection of fundamental liberties.

NB: The use of inverted commas around ‘predictive’ in this report serves as a reminder that so-called ‘predictive’ policing cannot truly or accurately foresee future events, such as crimes. Instead, it highlights that it is based on data-driven algorithms and statistical models that provide probabilities and trends, rather than definite predictions. Despite the assertions or wishes of tech enthusiasts, *Minority Report*-like prophetic certainty remains firmly within the realm of fiction.

URL: vaia.be/files/cursusmateriaal/presentaties/220617-3-Thomas-Marquenie.pdf

I. 'Predictive' policing by local police forces

In Belgium, the 'integrated police' (*geïntegreerde politie – police intégrée,* GPI) is structured on two levels: the Federal Police and 183 local police forces. While the latter are responsible for all basic police tasks, both judicial and administrative, the Federal Police provides them with various forms of support.

Several local police forces have used geographic 'predictive' policing and profiling systems, and participated in experimental 'predictive' policing schemes in recent years. There is little or no transparency in relation to these initiatives. It is possible that other police forces are also utilising 'predictive' systems or data profiling, or conducting similar projects.

In 2020, criminologists at KU Leuven conducted a survey of police forces in Flanders and the Brussels-Capital Region, which found that almost half of all police forces who responded used some form of data analysis. More precisely, 43% utilised 'manual data analysis', whilst 31% employed 'automated data analysis'.[3]

1. Orbit Geographic Information System (GIS)

The Geographic Information System (GIS)[4] produced by the company Orbit is the primary tool used by police forces in the Flanders and Brussels region. The company itself has claimed that its system is "already in place in nearly 100 police forces".[5] Orbit GIS offers the capability to spatially monitor historic crime reports, allowing for the identification of supposed geographic crime 'hotspots'.

Orbit also offers the 'Orbit Crime' tool for "crime analysis". The company gives the example of burglary, shoplifting, drugs (including trade and culture), nuisance and vandalism (illustrated by vandalism "committed by minors at a new construction site").[6] It offers further tools for "real-time visualisation" of "all staff and action plans of events in a single screen", and a specific tool focused on public order described as "negotiated management of public space".[7]

3 Lore Rooseleers and Jeroen Maesschalk. 2021. "Digitalisering in de lokale politie in Vlaanderen en Brussel: Waar staan we?" *Panopticon. Vol. 42, n° 5, p. 419-438.* URL: lirias.kuleuven.be/3611651

4 Orbit GIS. *Zones de police*. URL: web.archive.org/web/20230930192819/https://www.orbitgis.com/fr/zone-de-police NB: The program was rebranded as "Columba" in 2024. URL: www.columbasoftware.be/software/veiligheidsdiensten

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

6 Orbit GIS. *Zones de police – Stratégie*. URL: www.orbitgis.com/fr/zone-de-police/zp_strategie

7 Orbit GIS. *Zones de police – Outils opérationnels*. URL: www.orbitgis.com/fr/zone-de-police/zp_operationel

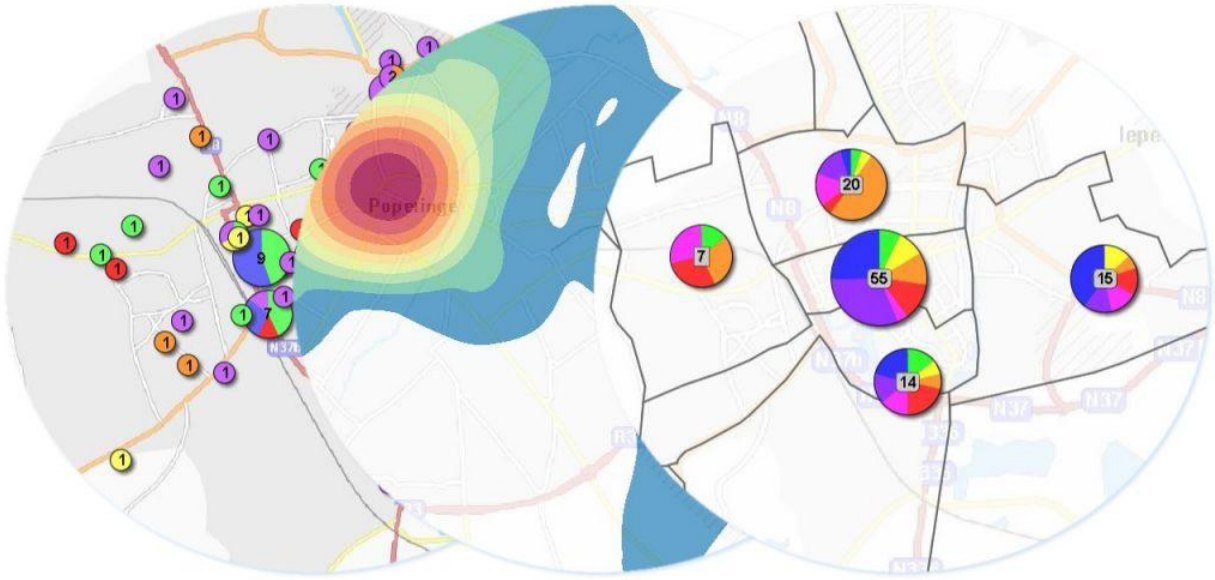

Figure 1. Screenshot from Orbit website showing 'Orbit Crime'
URL: www.orbitgis.com/fr/zone-de-police/zp_strategie

'Hotspot' policing has been shown in multiple contexts to perpetuate discriminatory patterns and excessive policing of particular individuals or areas, based on past interactions with law enforcement.[8] Despite this, several Flemish police forces have launched experimental trials of 'predictive' policing tools.

2. Westkust police force

The Westkust police force covers the Flemish municipalities of La Panne, Koksijde and Nieuwpoort. These are the communes bordering France, on the west of the Belgian coast. Only around 45,000 people live there, but the area attracts many tourists during the holiday period.

Figure 2. Panoramic photo of La Panne beach.
Copyleft Lokilech, 2008.

8 William Isaac and Kristian Lum, 'To Predict and serve?', *Royal Statistical Society*, 2016, DOI: 10.1111/j.1740-9713.2016.00960.x; Lyria Bennett Moses and Janet Chan, 'Algorithmic prediction in policing: assumptions, evaluation, and accountability', 2016, *Policing and Society*, 28:7, DOI: 10.1080/10439463.2016.1253695; Rashida Richardson, Jason Schultz and Kate Crawford, 'Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice', February 2019. 94, *N.Y.U. Law Review*. 192, URL: ssrn.com/abstract=3333423; Gizmodo, 2021. 'Crime prediction software promised to be free of biases, new data shows it perpetuates them', 2 December 2021, URL: gizmodo.com/crime-prediction-software-promised-to-be-free-of-biases-1848138977

The Westkust local police force was a forerunner of the police's digitisation process. It embarked on the implementation of 'predictive' policing systems as early as 2016.[9] Nicholas Paelinck, the local Chief Commissioner, personally visited Philadelphia in the United States to observe how police were deploying such systems there, and to see how they might be implemented in Westkust.

The stated aim of the local force is to have "less blue on the streets", meaning fewer patrols but more data analysts.[10] Speaking to the press, the Chief Commissioner explained how the project was intended to work:

> "We are already working with three data managers in our force. Through information they receive, we roughly predict where things could potentially go wrong. We then proactively send an intervention team there. It is not just about preventing burglaries, but the modus operandi also serves for preventive actions against quick thieves or drug dealers. The aim is to tackle crime before it happens".[11]

The actual operation of the programme has been described only in these general terms:

> "The police collect a wide range of data, from previous crimes to licence plates, court records and even the weather, and feed it into computers. Using algorithms, data analysts could suggest exactly where and when crimes might occur in the near future".[12]

The Chief Commissioner claimed that since the introduction of the Westkust programme, there has been a 40 per cent reduction in criminal incidents. The police claimed the 'predictive' capabilities of the software were most effective in tackling burglary and vehicle theft.[13]

However, the reliability of these unsubstantiated statistics must be called into question. No objective evaluations of the system are publicly available. Information regarding the computer programme used to conduct the analysis and make predictions or the allocate funds remains secret.

As the system evolves, the Chief Commissioner has also stated an intention to integrate the software with automatic number plate recognition (ANPR) cameras.[14]

In addition, the Chief Commissioner of Westkust is also the chairman of the Permanent Committee of the Local Police (CPPL-VCLP), the umbrella organisation of Belgium's local police forces. This means that he is well placed to spread the 'predictive' policing techniques he has tested in Westkust to police forces across the country.[15]

9 Rosamunde van Brakel. *Automating Society 2019: Belgium*. URL: algorithmwatch.org/en/automating-society-2019/belgium/

10 Haco. 'Politiezone Westkust experimenteert met datasets in strijd tegen criminaliteit'. De Standaard. 17/05/2016. URL: standaard.be/cnt/dmf20160517_02292901

11 MVHB. 'De toekomst van de politie: minder blauw op straat, meer blauw achter de computer'. *De Morgen*. 17/05/2016. URL: www.demorgen.be/nieuws/de-toekomst-van-de-politie-minder-blauw-op-straat-meer-blauw-achter-de-computer~bd35acda/

12 Haco. 'Politiezone Westkust experimenteert met datasets in strijd tegen criminaliteit'. *Op. Cit.*

13 *Ibid.*

14 Rosamunde van Brakel. *Automating Society 2019: Belgium*. *Op. Cit.*

15 CPPL, 2019. Memorandum 2019-2023. Commission Permanente de la Police Locale. pp. 5; 44-45.

3. Zennevallei police force

The Zennevallei police force covers the municipalities of Beersel, Halle and Sint-Pieters-Leeuw in the Flemish south-west suburbs of Brussels. In 2020, the force started a two-year project with Ghent University focused on the concept of 'predictive policing'. This approach involves the police force utilising 'predictive' insights to identify areas that pose a heightened risk for criminal activities, including burglaries and other crimes.[16]

Figure 3. Aerial view of Bergensesteenweg in Sint-Pieters-Leeuw
CC-BY-SA 3.0 Wouters Hagens, 2014

The police force announced that they won an award in 2022 for their initiative, stating:

> "In October 2019, the Zennevallei police force and UGent initiated a project to develop and practically test a big data policing model. The primary objective of the project was to address residential burglary, the most prevalent type of crime in Belgium, which has significant psychological repercussions on victims.
>
> The Zennevallei police force implemented the project between 2020 and 2021. Thus, risk maps were created through statistical models utilising big data to guide police patrolling proactively. In the short term, this allowed for risk assessments indicating the probability of crime, and subsequent deployment of resources in these high-risk regions. Over the long term, our objective is to attain more efficient police resource utilisation and crime reduction".[17]

URL: www.police.be/5806/sites/5806/files/downloads/Memorandum%20FR_0.pdf

16 EDRi. 'Use cases: Impermissible AI and fundamental rights breaches'. August 2020. URL: edri.org/wp-content/uploads/2021/06/Case-studies-Impermissible-AI-biometrics-September-2020.pdf

17 'Derde prijs voor Big Data Policing'. *Lokale Politie Zennevallei*. 18/03/2022. URL: www.politie.be/5905/nieuws/derde-prijs-voor-big-data-policing

The Zennevallei 'predictive' policing system has attracted the attention of the Belgian Senate, who questioned the Government on the matter. In response, the Minister of Interior indicated that it supported the Federal Police's efforts to improve its analytical capabilities and emphasised the fundamental importance of establishing a solid foundation for 'predictive' policing, including acquiring the necessary data. However, the Minister of Interior also acknowledged that police statistics predominantly reflect law enforcement activities and may not provide a comprehensive picture of the actual criminal landscape within a given jurisdiction.[18]

The Zennevallei programme was spearheaded by Anneleen Rummens, a doctoral student from Ghent University, under the supervision of criminology professor Wim Hardyns. They gathered extensive 'big data' encompassing a range of variables. This included location and time, as well as additional factors such as weather conditions during specific incidents. The intention was to meticulously map out this intricate web of information.[19]

Their method is based on Risk Terrain Modelling (RTM), a spatial 'predictive' policing method that draws on geographic information systems (GIS) and criminological theory to attempt to identify areas potentially at higher risk of criminal activity. RTM is based on the premise that specific environmental factors, known as 'risk terrains', influence criminal incidents.

However, RTM has attracted considerable criticism due to the criminological theories that underpin it.[20] The fundamental theory behind RTM is that certain geographical areas inherently attract or generate criminal activity.[21] This assumption lacks empirical support. Crime is the result of a complex interplay of various social, economic and individual factors. By emphasising geographical factors, RTM tends to overlook the underlying socio-economic, cultural and structural causes of crime.

Moreover, RTM's focus on geographic factors may inadvertently reinforce spatial bias, by disproportionately targeting certain neighbourhoods based on historical crime data. This can perpetuate over-policing in disadvantaged communities, exacerbating existing inequalities. As anti-colonial geographer Brian Jefferson explains:

> "The effects of police bias, jury bias, and sentencing bias on crime patterns are not systematically explored in any of these techniques. Nor do these techniques address how laws, policies, or police practices influence the geographic patterns found in crime data. Crime maps do not offer definitive, objective pictures of illegal behaviors so much as they raise questions about how such behaviors are monitored and recorded".[22]

18 Minister of Interior's answer of 09/07/2020 to written question n°7-591. *Belgian Senate*. URL: senate.be/www/?MIval=/Vragen/SVPrintNLFR&LEG=7&NR=591

19 Anneleen Rummens & Wim Hardyns. 2020. 'Comparison of near-Repeat, Machine Learning and Risk Terrain Modeling for Making Spatiotemporal Predictions of Crime'. *Applied Spatial Analysis and Policy*, Vol. 13, no. 4, pp. 1035–1053. DOI: 10.1007/s12061-020-09339-2

20 Brian Jefferson. 2020. 'Crime Mapping'. In: *International Encyclopedia of Human Geography*. Elsevier. pp. 11-15.

21 Henri Buccine - Schraeder & Leslie W. Kennedy, 2021. 'Risk Terrain Modeling (RTM)'. In: *The Encyclopedia of Research Methods in Criminology and Criminal Justice*, edited by J.C. Barnes & David R. Forde, Wiley, pp. 873–74. Wiley, 2021. DOI: 10.1002/9781119111931.ch169

22 Brian Jefferson. 2020. 'Crime Mapping', *Op. Cit.*, p. 14.

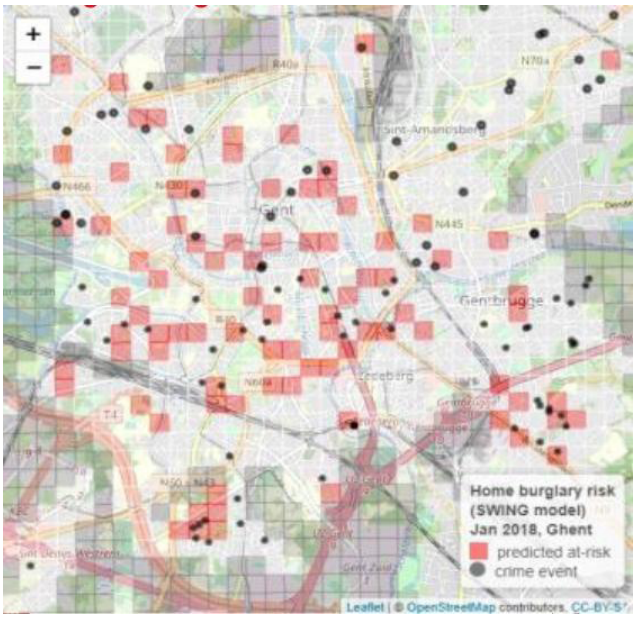

Figure 4. Predicted burglaries (red squares) *vs.* actual burglaries (black dots) in Ghent
Source: Rummens & Hardyns. CPS international conference 'Street policing in a smart society'. 17/09/2019.

As a result of their research, the Ghent University researchers Hardyns and Rummens came to the conclusion that:

> "Predictive policing can enable a more focused use of data to achieve a data-driven operation within police forces. In addition to novel data sources, implementing new methods like machine learning can provide dynamic insights into how crime patterns develop. Nevertheless, numerous data sources and related methods remain largely unexplored. For example, social media data and new methods within the broad field of machine learning (*e.g.* deep learning models, the advanced version of neural networks) could be considered. Currently, the potential of exploring these novel sources and methods has yet to be realised".[23]

Hardyns and Rummens appear to show little concern for the potentially discriminatory consequences of the system they developed, particularly given the abundance of sensitive data that it uses. Speaking at a conference, Hardyns attempted to mitigate concerns around discrimination by emphasising the alleged neutrality of technology.[24] The argument for technological neutrality goes as follows: technology is not inherently good or bad; instead, its ethical worth depends on its use. The argument, however, is easily refuted. The potential for harm is heavily determined by the technical characteristics of a certain technology, as their production is inherently embedded within their social context and goals. Illustrating his supposedly neutral stance, Hardyns claims that: "Guns don't kill people. Stupid people with guns kill people".[25]

23 Wim Hardyns & Anneleen Rummens. (2021). Predictive policing: een balans na zes jaar empirisch evaluatieonderzoek in België. Tijdschrift voor Veiligheid (20) 4, 9-23. URL: tijdschriften.boomcriminologie.nl/tijdschrift/tijdschriftveiligheid/2021/4/TvV-D-21-00005

24 Wim Hardyns. Academic panel session: Predictive policing in the big data era. *CPS International Conference 'Street Policing in a Smart Society'*. 17/09/2019. URL: policingandsecurity.be/wp-content/uploads/2020/05/2019-09-17_Studiedag_Street-policing_Hardyns_Academic-panel-session.pdf

25 *Ibid.*

Hardyns' team also recently looked at crime statistics in Brussels and tried to identify patterns. Their research led them to make a series of recommendations that flow with the 'predictive' tide. They call for more big data and automated analysis, as well as the integration of multiple surveillance and data sources:

> "Crime in Brussels is more related to the mobility of offenders and thus perhaps necessitates offender-focused approaches aimed at targeting the mobility of offenders in real-time, *e.g.,* using Automatic Number Plate Readers *(*ANPR) or surveillance systems. In general, it could therefore be beneficial to regularly monitor and analyse the crime data and thus to implement a more real-time Intelligence-Led Policing approach in general. In that regard, it could also be recommended to combine place-based and person-based policing approaches or to apply more dynamic policing approaches that might enable to take into account the level of crime concentration, the spatial (in)stability of crime, the mobility of offenders and real-time information (*e.g.,* place-based predictive policing approaches). [...]
>
> Additionally, it is crucial to explore the potential integration of alternative (big) data sources with official police records. Incorporating relevant information from sources like social media (*e.g*., Twitter data) and employing text mining techniques can provide qualitative insights into crime-related incidents. This could enrich our understanding of crime concentrations and contribute to more comprehensive and innovative analyses".[26]

Given Hardyns' influence in the field of 'predictive' modelling for law enforcement, it will be important to follow future research conducted by him and his team. In 2023, he was awarded nearly €2 million by the EU to carry out a five-year project, BIGDATPOL.[27] The research goal is to "integrate statistical-methodological, criminological, legal and ethical conditions into a single evidence-based 3D model." This is supposed to provide "both academia and law enforcement practice with guidelines and recommendations for studying, applying and implementing big data policing".[28] Hardyns and his team have also worked with statistics from the Antwerp police, discussed in the following sub-section.

4. Antwerp police

Antwerp is the second largest city in Belgium but has only one police force. Brussels, the capital city, has six separate police forces. This makes the Antwerp police one of the largest and most important forces in the country.

This is compounded by the fact that Belgian police forces are governed by the local municipality. The Antwerp municipality was run from 2013 to 2025 by Bart De Wever, the leader of the right-wing Flemish nationalist party the New-Flemish Alliance (N-VA). De Wever is one of the most influential politicians in Belgium, currently serving as the Prime Minister (2025).

26 Robin Khalfa, Thom Snaphaan, Lieven Pauwels, Ourania Kounadi and Wim Hardyns, 2023. 'Crime within a Bandwidth: Testing "the Law of Crime Concentration at Place" in Brussels'. *European Journal on Criminal Policy and Research*. DOI: 10.1007/s10610-023-09556-8.

27 'Towards an evidence-based model for big data policing: Evaluating the statistical-methodological, criminological and legal and ethical conditions'. *Cordis EU research results*. 2023. DOI: 10.3030/101088156

28 'Six Ghent University researchers win ERC Consolidation Grant'. *UGent. 31/03/2023.* URL: web.archive.org/web/20230814224751/https://www.ugent.be/en/news-events/six-ghent-university-researchers-win-erc-consolidator-grant

Figure 5. Cityscape of Antwerp
CC-BY-SA 3.0 Paul Hermans, 2012

A number of public procurement contracts signed by the Antwerp police have subsequently been extended to other police forces. This demonstrates the influence of Antwerp police in the wider digitisation and automation of policing in Belgium.

Antwerp has signed a €2,000,000 contract with the Swedish corporation Securitas[29] to privatise certain police functions, such as the surveillance of public events and strategic perimeters or open-street CCTV monitoring.[30] The same contract allows for the purchase of equipment. Many Belgian police forces have signed up to buy body-worn cameras through it.

In addition to the Securitas technologies, Antwerp police has developed its own smartphone application called FOCUS, which gives police officers access to police databases. The app has been sold by the Antwerp police to the integrated police and largely rolled-out across the country.

The standard FOCUS application, accessible to each Belgian police force, has multiple modules. These include:

- the 'Search' module, giving officers access to all available databases. The module also proactively provides information. When officers search for a location, the app automatically retrieves data on individuals (and possibly weapons) registered at that address, as well as previous incidents;
- the 'Incidents' module provides officers with an up-to-date overview of ongoing events in the field;
- the 'ISLP' module (Integrated System for the Local Police) allows officers to quickly create reports on the ground;

29 Securitas Security company. URL: www.securitas.be
30 Lokale Politie Antwerpen. LPA/2017/295. URL: enot.publicprocurement.be/enot-war/preViewNotice.do?noticeId=319270

- the 'Messages' module offers a platform for police officers to communicate with one another;
- the 'Images' module enables officers to take and upload photos;
- the 'Maps' module features multiple map layers including: the location of field units, CCTV cameras, and an overview of the real-time traffic situation.

In addition to the core package, police forces have the option of adding additional modules to the FOCUS application.[31]

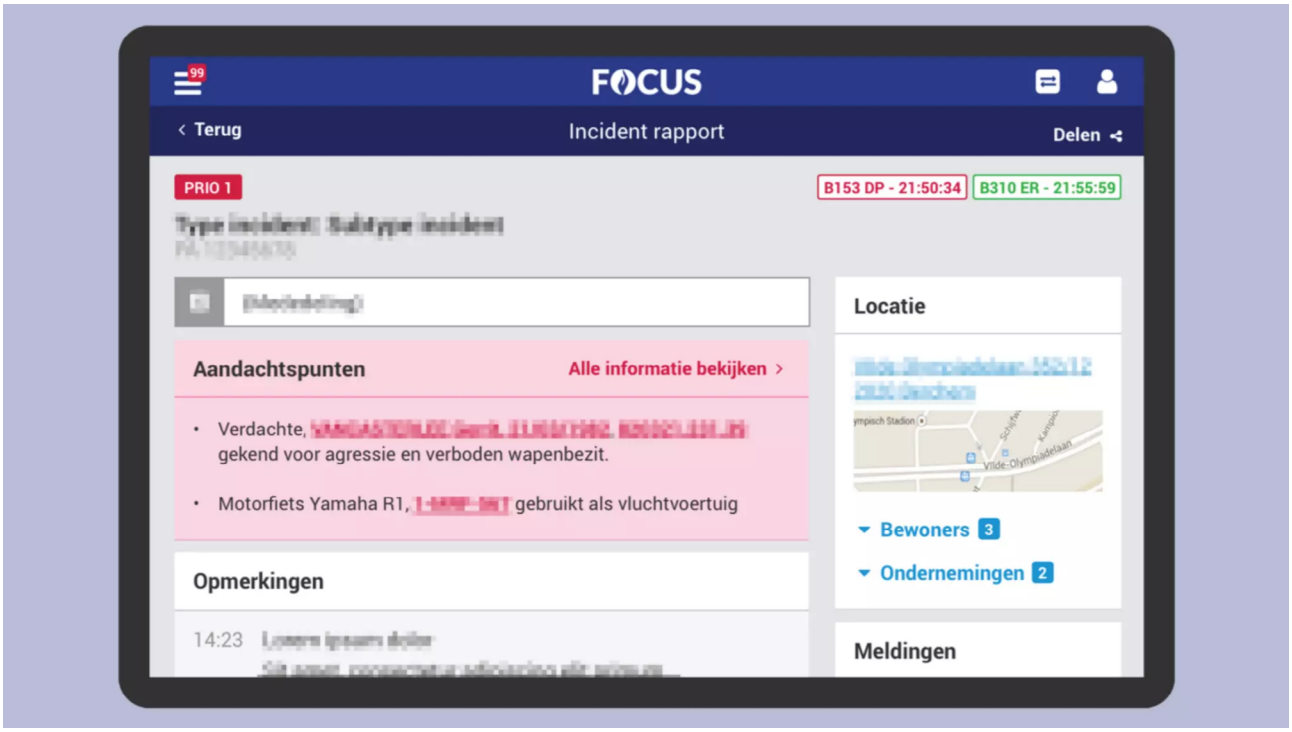

Figure 6. The FOCUS app user interface
Source: Monkeyshot. 2018. 'A typical user research for the Antwerp police force – IxD18'. *Slideshare.*

The FOCUS system also features an algorithm that allows police forces to collate data from a diverse range of sources including: the main police database (BNG-ANG); the ANPR and licence plate register (DIV); and the 'Integrated System for Local Police' (ISLP). Using data from the ISLP raises particular concerns. The information held on this database is unverified and mostly consists of uncorroborated field notes taken by police officers, largely based on hearsay and opinion.

Another software platform used by Antwerp police aggregates data from ANPR systems, police car locations, CCTV cameras and crowd management via mobile phone tracking.

Antwerp police have also applied advanced analytics techniques, including text recognition, human parsing, behavioural profiling and object tracking, to CCTV images.[32]

31 Lore Rooseleers and Jeroen Maesschalk. 2021. 'Digitalisering in de lokale politie in Vlaanderen en Brussel: Waar staan we?' *Op. Cit.*
32 Jo Forceville. 2023. 'Big Data en politie, evolutie in versnelling: Een blik voorbij data en technologie'. In Snaphaan *et al. (eds.). Cahiers Politiestudies. no. 66: Big Data Policing. Antwerpen: Gompel&Svacina. pp. 107-120.*

Jo Forceville, a 'smart policing' specialist at Antwerp police, foresees a transition towards artificial intelligence (AI) and open-source intelligence (OSINT) methodologies:

> "There are ongoing projects on social media scraping, deep learning models and the use of AI in the analysis of camera images. Social media scraping is used in radicalism investigations, for example, to look for suspicious patterns or routes in traffic".[33]

Clearly, Antwerp is a leader in the implementation of new technologies. It will be important to maintain scrutiny of the city's police force to stay updated on developments in the use of technology by the Belgian police.

33 *Ibid.*

II. Belgian police databases

Police databases serve as the primary data source for 'predictive' policing and data-profiling systems. Therefore, it is necessary to describe their uses and contents.

Police databases in Belgium are officially divided into five categories:

1. The National General Database (BNG-ANG);
2. Basic databases;
3. Special databases;
4. The common database (CDB);
5. Technical databases.

Private data sources, especially social networks and geolocation data provided by telephone operators,[34] also play a significant role and will be covered further.

1. Brief presentation of the different types of database

a. The National General Database (bng-ang)

The National General Database (*Banque de données Nationale Générale – Algemene Nationale Gegevensbank,* BNG-ANG hereafter) is the main police database and is divided into three sections: traffic; administrative; and judicial police. This database is accessed frequently for police investigations. In 2019, the bng-ang contained information about a staggering three million people – a quarter of the Belgian population.[35] The reliability of this information varies and may concern suspects, witnesses or victims, and may relate to any type of incident. Since 2019, the repressive measures associated with the covid pandemic have certainly not reduced this figure.

The Supervisory Body for Police Information (COC) recently published a caustic report on the utilisation of the BNG-ANG.[36] Official protocol stipulates that unverified data must be checked by a second party before being added to the BNG-ANG. Despite this, there are cases of dubious information being stored in the database.

34 Corentin Debailleul. 2021. 'Pistage dans le cyberespace'. *Culture & Démocratie*. no. 53. URL: www.cultureetdemocratie.be/articles/pistage-dans-le-cyberespace

35 Olivier Bailly. 'BNG, la base non gérée'. *Médor*. 14/04/2021. URL: medor.coop/hypersurveillance-belgique-surveillance-privacy/police-justice-bng/episodes/bng-la-base-non-geree-25

36 COC, 2023. *Rapport concernant les infractions commises par des membres de la police intégrée dans le cadre de traitements dans la bng*. Organe de contrôle de l'information policière. DIO23001. URL: www.organe-decontrole.be/files/DIO23001_F.pdf

There is a culture of presumed legitimacy surrounding police database searches, and a degree of leniency is sometimes shown to officers who overlook the protocol. The police have only recently initiated archiving procedures to remove outdated data, something they are legally required to do.[37] As is often the case when the police stray from the legal path, penalties are weak or non-existent. This is how the COC explains the situation:

> "As a member of Committee P [Permanent Oversight Committee on the Police Services] in 2007 or 2008, I carried out a study, an analysis of all the sanctions and sentences handed down to police officers, and it became clear that police officers were in fact judged very lightly, both by the investigating districts and very often no prosecutions were brought".[38]

A Belgian lawyer and legal scholar, Catherine Forget, has observed that "the bng-ang archives data for thirty years before deletion. However, it should be noted that in principle, data processed in police and judicial databases should be archived when deemed inadequate, irrelevant or excessive, irrespective of retention periods".[39]

In practice though, data retention periods are often greatly exceeded, resulting in the indefinite storage of data without archiving or deletion.[40] The present data protection officer (DPO) of the police force of Charleroi said that upon his appointment in 2014, he was faced with thousands of unfinished procedures in the BNG-ANG that needed to be completed. It took several years to eliminate the backlog.[41]

B. Basic databases

Basic databases are used by the integrated police to record the field notes taken by police officers during their operations. They cover the data processed for administrative and judicial police purposes, including penalty notices and reports relating to events, which can encompass a broad range of situations.

The BNG-ANG is fed by records from the basic databases. This is done using applications such as:

- ISLP (Information System for the Local Police), which is used to encode official reports;
- FEEDIS (Feeding Information System) for the Federal Police; and
- GES/Itinera, which "offers all federal investigation services the possibility of consulting, almost in real time, the status of their cases with the Justice Department".[42]

37 COC, 2023. DIO23001. *Op. Cit.*
38 Hearing of the COC at the Federal Parliament following his report on the BNG-ANG. 28/06/2023. *Chambre des représentants de Belgique*. Doc 55 3467/001.
39 Catherine Forget. 'L'effacement des données policières et judiciaires : un parcours du combattant ?'. *e-legal, Revue de droit et de criminologie de l'ULB*, vol. 6, March 2022. URL: e-legal.ulb.be/medias/pdfs/178-l-effacement-des-donnees-policieres-et-judiciaires-un-parcours-du-combattant.pdf
40 *Ibid.*
41 Interview with the DPO of Charleroi police force. 03/07/2023.
42 Police Fédérale. 'La gestion de l'information au cœur de notre organisation'. *2017 Annual Report of the Federal Police*. URL: police.be/5998/sites/5998/files/downloads/RA2017_web_FR.pdf

c. Special databases

Special databases are created and used by police departments for specific, designated purposes. According to the Police Act:

> "Heads of local police forces; the General Commissioner; and Directors may create, for specific purposes, special databases for which they are data controllers, with the aim of processing the data contained therein in the exercise of their administrative and judicial police duties and purposes".[43]

Regarding the areas that special databases actually cover, the COC chair explains:

> "It can be anything. For example, youth gangs, they are certainly present in the Brussels area. There are six local police forces in the Brussels region, probably all of them have a database on youth gangs, or have a database on terrorism and/or radicalisation. So all those are, for example, known people for burglary, repeat offenders. Those are all possible databases when it comes to special databases".[44]

These databases are frequently used at the local level, but the Federal Police also utilise them. For example, the administrative branch of the Federal Police is responsible for monitoring protests and uses special databases for alleged far-right and far-left activists.[45]

Many of these special databases exist off the radar. They can even operate beyond the oversight of the COC, whose head stated:

> "I think there are about 1600 of those databases that we know of. But I do not know, evidently, every particular database. There is, in principle, no system of direct access, certainly not direct access to special databases. But here, it is ultimately the local police chief who decides who can have access or not. [...] That is the big difference between the three kinds of databases. For the basic databases and for the general database, [those] responsible in terms of data protection are the Ministers of Interior and Justice, but for the local, for these special databases, it is the local police chief or director. [...] So for us, it is evidently much more complicated to have a good view on those particular databases. There is only one way to know and that is going to the local police force and asking them to show us".[46]

The COC has also criticised the lack of oversight and accountability of special databases:

> "Regarding special databases, I think it is a real problem because most of them are not logged. The police forces that are trying to do this properly, are trying to get it right as they go along. The systems are very specific and it may just be an Excel file, so these logins are very different, but for us it is going to be a big problem in the future, so it's important to get it in order, and at the moment it is not in order at all".[47]

43 Art. 44/11/3 of the Police Act. URL: ejustice.just.fgov.be/eli/loi/1992/08/05/1992000606/justel
44 Interview with Frank Schuermans (COC), 17/02/2023.
45 Interview with police union delegates, 17/08/2023.
46 Interview with Frank Schuermans (COC), 17/02/2023.
47 Hearing of the COC at the Federal Parliament following his report on the BNG-ANG. 28/06/2023. *Chambre des représentants de Belgique*. Doc 55 3467/001.

Regarding the opportunity to use such databases, the COC is quite explicit:

> "When we do proactive audits, we will always go and say look, "give me a list of all your special databases, explain to me why it is necessary to have those databases". And in 99% of the cases when we start off with, for example, 25-30 special databases, [but] when we have left or when our inquiry is finished, half of them will be gone".[48]

This point of view was also confirmed by the DPO of Charleroi police. Perhaps unsurprisingly, their view is that the BNG-ANG possesses several advantages: it is accessible to other police forces, is better governed and monitored, and data entered in the system must be validated. He asserts that special databases are only worthwhile in exceptional cases. For instance, the BNG-ANG does not allow uploads of high-definition images. On the whole, however, the DPO for the Charleroi police views the BNG-ANG as the preferred option.

From a human rights perspective, the question is rigged: both forms of police databases present considerable risks. Choosing between an extraordinarily large centralised national database and poorly managed local databases is akin to choosing between a rock and a hard place. These risks will be addressed in a subsequent section of this report.

d. The Common Database 'Terrorism, Extremism, Radicalisation Process' (CDB T.E.R.)

The CDB T.E.R. allows the police and intelligence services to share information, with a focus on counter-terrorism. According to the database operator, the Coordination Unit for Threat Analysis (CUTA), the common denominators of all individuals included in the CDB T.E.R. are 'extremism', 'terrorism', or 'potential for violence'.[49]

The CDB contains five categories, defined as follow:

- "Foreign Terrorist Fighters (FTF): persons who have travelled to a conflict zone in order to join a terrorist group or have returned from a terrorist conflict zone, who have been prevented of leaving or who intended to leave;
- Homegrown Terrorist Fighters (HTF): persons who do not intend to travel to a terrorist organisation abroad. They choose to commit or support terrorist acts here;
- Hate propagandists (HP): persons who want to justify the use of violence for ideological purposes. With their influence, they aim to radicalise their environment and undermine the rule of law;
- Potentially Violent Extremists (PVE): persons with extremist sympathies who intend to convert these into actions through violence, but who have not yet taken concrete steps to do so;

48 Interview with Frank Schuermans (COC), 17/02/2023.
49 'The Common Database (CDB)'. *CUTA*. URL: cuta.belgium.be/the-common-database-cdb

- Persons Convicted of Terrorism (PCT): persons who are convicted of terrorism, interned or placed under specific protective measures for terrorism in Belgium or abroad".[50]

While some categories are clearly defined, others are largely open to interpretation. The Committee for Vigilance in the Fight against Terrorism (Committee T) denounces the gradual extension of the CDB T.E.R. to ever broader and ever more vague categories.[51] This is all the more problematic as this database can be used to grant or deny security clearances.[52]

In 2022, there were approximately 700 individuals on the CDB T.E.R. The authorities claim that 87% of those on the database "subscribe to a jihadist ideology", 10% are right-wing extremists, and 2% are left-wing extremists. Others on the database include "various threats" including "anti-establishment sentiments arising from the Covid-19 pandemic or a political context abroad".[53]

E. Technical databases

The final category of police databases, so-called 'technical' databases, stands apart from the others. These hold personal data and information that is collected automatically – at present, exclusively through automatic number plate recognition (ANPR) cameras. These ANPR cameras have direct access to the Vehicle Registration Service (DIV), enabling the identification of specific vehicles of interest, such as stolen or uninsured cars.

The COC recently stated that "for the operation of ANPR, we cannot see who has consulted this data at what time, there is no log, which in fact poses a juridical problem"[54] – an understatement to say that it's illegal.[55]

50 *Ibid.*
51 Comité T. Rapport 2021. *Comité de vigilance en matière de lutte contre le terrorisme*. pp. 18-20. URL: comitet.be/wp-content/uploads/2021/03/Comite-T-Rapport-2021-Verslag.pdf
52 Arrêté royal du 8 mai 2018 déterminant la liste des données et informations qui peuvent être consultées dans le cadre de l'exécution d'une vérification de sécurité. URL: beroepsorgaan.be/images/boor/6_1/Veiligheids_verificaties_gegevens.pdF
53 "700 extrémistes font l'objet d'un suivi prioritaire dans notre pays". *OCAM-OCAD*. 28/07/2023. URL: ocam.belgium.be/700-extremistes-font-lobjet-dun-suivi-prioritaire-dans-notre-pays Europol has similar concerns at the European level. See URL: www.statewatch.org/news/2021/june/eu-growing-online-censorship-of-presumed-violent-extremism-of-all-ideological-varieties
54 Hearing of the COC at the Federal Parliament following his report on the BNG-ANG. 28/06/2023. Chambre des représentants de Belgique. Doc 55 3467/001.
55 See DGPR, article 25. URL :eur-lex.europa.eu/eli/dir/2016/680/oj#art_25

Figure 7. A Macq ANPR camera (left) and official signage (right) in Saint-Gilles, Brussels-Capital Region.
Photos by Corentin Debailleul, CC-BY-SA.

ANPR cameras occupy a significant role in Belgian surveillance efforts. They are justified by a spectrum of reasons, from anti-terrorism to the enforcement of low-emission zones (LEZ). Their ambiguous purpose raises concerns about function creep – *i.e.* the expansion of a technology beyond its original purposes. Indeed, the Brussels ANPR was simultaneously announced as a counter-terrorist measure and as part of the LEZ, with the aim of combating pollution and improving health. However, permissions were soon granted for their usage in the enforcement of pedestrian areas too.

Intertwining video analytics with technical databases, ANPR cameras represent a pivotal precedent. It would be particularly alarming if the same kind of connection were extended to face recognition – which would amount to a systematic identity check on all passers-by.

2. The risks associated with police databases: case studies

Police databases carry grave potential for discrimination due to the categories used, the information held, and the lack of regulation around their existence, use and content. As criminologist Jan Van Dijk puts it, police data "reflect[s] the crime problem as perceived by law enforcement agencies and the politicians, prosecutors or judges who oversee their work." These institutions are "subject to their own biases".[56]

According to the Police Act, the BNG-ANG, basic databases and special databases can be used to process the personal data of individuals in specific categories for

56 Van Dijk. 2009. 'Approcher la Vérité en matière de délinquance: La comparaison des données d'enquêtes en population générale avec les statistiques de police sur la délinquance enregistrée'. In: *Mesurer la délinquance en Europe*. L'Harmattan. Quoted in: Rémy Farge, 2020. 'Police du futur et nouvelles technologies du profilage ethnique'. *La chronique des droits humains*. pp. 13-16.

administrative policing and judicial policing purposes.[57]

For administrative purposes, this includes:

- the contact information of organisation representatives;
- individuals involved in public order incidents;
- national or international group members who pose a threat to public order;
- individuals who are likely to cause harm to others or property that requires protection; and
- individuals subject to an administrative measure issued by a competent administrative authority and placed under police surveillance.[58]

Lawyer and researcher Catherine Forget describes the harmful consequences that may arise if information is held about an individual on a police database:

> "This matter pertains to any individual who is known to the police when certain details regarding them are logged in databases, possibly without their awareness or without them ever having been involved in criminal proceedings. This logging can not only create a sense of confusion but can also result in unpleasant or even distressing circumstances for the affected individual. They could be made to undergo enhanced identity checks at the airport, which may include questioning, or be subjected to unwarranted searches. They may also be unable to obtain a security certificate for their professional activities, thus being effectively prevented from performing their job".[59]

Data held on these databases may seem innocuous, but it can have serious consequences. In their 2022 annual report, the COC comments that:

> "The quality (accuracy and precision) of police databases still leaves a lot to be desired, with potentially very damaging repercussions for citizens. Citizens can be directly or indirectly harmed by incorrect, outdated or otherwise inappropriate data processing. Directly, because the processing to which the citizen is subjected (search, arrest, police approach, link with ANPR technical databases, etc.) cannot be correct if it is based on incorrect information. And indirectly, because access to certain professions is unfairly hindered or blocked [...] security guards, military personnel, private security workers, nuclear power plant workers and others are all judged on the basis of their 'police record'."[60]

Several cases noted by Committee P, the Oversight Committee on the Police Services, revealed that this information was being used without adequate precautions.[61] For example, one case involved information that an individual was

57 Art. 44/5 of the Police Act.

58 Catherine Forget. 'L'effacement des données policières et judiciaires : un parcours du combattant ?'. *e-legal, Revue de droit et de criminologie de l'ULB*, vol. 6, March 2022. URL: e-legal.ulb.be/medias/pdfs/178-l-effacement-des-donnees-policieres-et-judiciaires-un-parcours-du-combattant.pdf

59 *Ibid.*

60 COC. *Rapport d'activité 2022*. Organe de contrôle de l'information policière. URL: organedecontrole.be/files/Rapport-dActivit%C3%A9_COC_2022.pdf

61 Rosamunde van Brakel. 2021. 'How to Watch the Watchers? Democratic Oversight of Algorithmic

purportedly HIV-positive and allegedly planned to infect police officers during an operation. The inquiry undertaken by Committee P and the COC discovered that the information derived solely from hearsay, with no legal or administrative grounds for its storage. The information was not evaluated comprehensively, and there was no tangible reason to store it in the database.[62]

Since the adoption of a 2019 reform,[63] law enforcement agencies are authorised to handle particular categories of data, including sensitive data like health, biometric, and genetic data, as part of their administrative and legal policing duties, as well as in the context of international police cooperation. Biometric data refers to personal data relating to physical or physiological characteristics of an individual. For example, it includes fingerprints, facial features, vocal patterns, and earprints. The gathering of such information requires careful handling due to the risks related to disclosure of sensitive information, such as a person's ethnicity or health.[64]

We will now examine several case studies to illustrate specific risks associated with the use of police databases. We will firstly examine special databases, for sex workers on the one hand and urban 'gangs' on the other. Then, we will delve into so-called anti-radicalisation policies, screenings, and security clearances. Finally, we will conclude this section by examining recent judicial litigation that could challenge the current approach in Belgium for individuals' right to access their police files.

a. Sex worker databases and profiling

Since 2022, sex work has been decriminalised in Belgium.[65] The provision of sexual services was never forbidden *per se,* but incitement and procurement were criminalised. Additionally, there used to be a form of indirect criminalisation. This meant that anyone making money from sex work, even at many degrees of separation, was considered a procurer. Consequentially, a room-mate, a chauffeur, an accountant, etc. could be convicted of procuring.[66]

What remains criminalised is the trafficking of human beings, as well as certain forms of procurement considered abusive. Nevertheless, the federal system of government in Belgium allows local authorities significant discretion in their regulation of the industry. Various local regulations often set restrictions on the performance of sex work.

Police Surveillance in Belgium'. *Surveillance & Society, vol. 19, no. 2, pp. 228-240.* URL: ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/14325/9779

62 Rapport d'activité 2003 du Comité permanent de contrôle des services de police. *Chambre des représentatns de Belgique et Sénat*. 30/07/204. URL: comitep.be/document/jaarverslagen/2003.pdf

63 Loi modifiant diverses dispositions en ce qui concerne la gestion de l'information policière. Moniteur Belge. 22/05/2019. URL: www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=19-06-19&numac=2019013125

64 Catherine Forget. 'L'effacement des données policières et judiciaires : un parcours du combattant ?' *Op. Cit.*

65 Loi modifiant le Code pénal en ce qui concerne le droit pénal sexuel. Moniteur Belge. 21/03/2022. URL: www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=22-03-30&numac=2022031330

66 Interview with the coordinator of an association supporting sex workers in Brussels, 04/08/2023.

In Antwerp for instance, sex work is mainly concentrated in a specified district, the *Schipperskwartier*. A police team of 15 members, known as the *prostitutieteam*, is responsible for monitoring this area. The police conduct inspections of sex work locations and initiate criminal proceedings for the most severe offences, such as alleged human trafficking. However, for minor offences such as noise pollution, the city intervenes by enforcing measures such as administrative sanctions, fines, or closures if there are acts of nuisance or other disruptions to public order (including health, safety, and tranquillity).

In 2020, Antwerp developed a platform called 'HookUp' to monitor 'window' sex work. The stated aim of HookUp is to prevent the coercion of sex workers and interference from intermediaries. HookUp is a platform for the owners and/or managers of sex work establishments, and for sex workers themselves. Creating a profile on the HookUp platform is a compulsory requirement for individuals seeking to rent a workspace in the *Schipperskwartier*. Similarly, there are requirements for a certificate of aptitude and specific licenses to rent out an establishment to sex workers. To obtain these, applicants must provide their information in the HookUp application form, which is stored for up to five years.

The application gathers and passes on data to the local authorities, including information on the locations where sex workers operate, and ownership of premises. The city's website states that information regarding sex workers is accessible solely to the police, supposedly for the purpose of guaranteeing their safety.[67]

HookUp offers the police insights into completed rental agreements, is meant to provide a platform for sex workers to report abusive conduct, and also serves as a means for the police to share information, such as the photograph of perpetrators of sexual violence. Additionally, the police use the platform to confirm the identity of new sex workers, collaborating with the city for the supposed purposes of addressing subletting, human trafficking, and other activities defined as criminal.

However, the police also use this data for different objectives. Clearly, on the face of it, guaranteeing the safety of sex workers and combating human trafficking are positive aims. But when this is undertaken through surveillance and monitoring, sex workers may be subjected to greater risks, especially those who are most vulnerable.

Because the platform is monitored by the police and registration is compulsory, people with irregular or precarious migration status are excluded from it. Anthropologist Anna Di Ronco, who researched the policing of sex work in Antwerp, writes:

> "Identified sex workers are approached by the police pretending to be clients and are then recorded in the police database during an administrative inspection carried out in tandem with the city. During these administrative inspections, the regular status of migrant sex workers is also carefully checked by the police (for example: 'sometimes when they are illegal – we are still police so we have to do our job [...] it has to be investigated whether they can stay in Belgium or not')".[68]

67 'Prostitutiebeleid'. *Stad Antwerpen*. URL: www.antwerpen.be/prostitutiebeleid

68 Anna Di Ronco. 2022. 'Law in action: Local-level prostitution policies and practices and their effects

As Di Ronco recounts, compulsory registration of sex workers on the HookUp app pushes migrant sex workers in Antwerp to less-visible spaces. Here, they are less likely to be supported by social organisations:

> "Repressive police actions on the streets have also led sex workers, especially non-EU migrant sex workers without a visa, to move indoors and use online websites and apps, thus making it much harder for social workers to reach out to them. When commenting on Antwerp's prostitution policy, one social worker suggested: [I]t pushed some sex workers to the margins, and even with the best intentions [...] Trying to control too much is always pushing people more to invisible spaces, like rooms, apartments, the Internet, where of course for us as a social organization it is more difficult to reach them".[69]

This contrasts markedly with the situation in Brussels, where police appear to be less concerned with the migration status of sex workers. The coordinator of a local association supporting sex workers described the relations between sex workers and the police in the Yser neighbourhood, located between the city centre and the North Station:

> "There is a big difference between what they call the 'Playmobils' and the plain-clothes agents. The plain-clothes ones are from the vice squad while the 'Playmobils' are just ordinary guys from Brussels local police... Basically in the vice squad, the cops have a very paternalistic relationship with the sex workers in Yser. But it is a give and take, in other words, they come and say: "How are you? Are there people bothering you? Are there guys robbing you? Are there any drugs? Are there any pimps around?" They are fishing for information. [...] We trust the vice squad; they do not really care about undocumented migrants. It is not their problem. Their problem is racketeering, [...] that is what the vice squad is interested in, and that is where their interest lies, getting to know the girls, finding out where they work and getting them to tell them what is going on. [...] The local cops are terrible because they change from week to week. One week they will leave you alone, the next week they will ask you: "Come on, move"... [...] So the city cops are very unpredictable. [...] Actually, in Yser, all the girls are asking is: "We do not care if the police come to see us, we just want to know, we do not want to be told something different every week".[70]

Therefore, the decriminalisation of sex work significantly improves living conditions for sex workers and reduces the likelihood of migrant sex workers being investigated. However, while decriminalisation is widely supported, opinions are less clear when it comes to the regulation of sex work. For instance, some grassroots initiatives have long campaigned for the recognition of an official status for sex workers, while others are less enthusiastic about the matter. A local social worker recounts:

> "99.99% of the people we see do not give a fuck about sex worker status. They do not have papers, they do not have a shelter, they do not have health insurance. So when we tell them that you can have official sex worker status, they say: "but I don't even have papers, I don't give a damn". So I am happy that they can have a status if that is what sex workers want. But I do not endorse it because I am not a sex worker and that is not what the people

on sex workers'. *European Journal of Criminology*. Vol. 19, no. 5, pp. 1078-96. DOI: 10.1177/1477370820941406.

69 *Ibid.*

70 Interview with the coordinator of an association supporting sex workers in Brussels, 04/08/2023.

> we see want. So all these questions about whether I should declaremyself a sex worker or not, we do not see a lot of that here. Hence I think to myself, knowing that in Antwerp the profile of people is more or less the same [...] I imagine that the application in question in Antwerp [HookUp], if you do not have a national number, if you do not have papers, I don't know if you are going to register on it".[71]

A new Federal Law was passed in 2024[72] that aims to provide protections for sex workers. However, it also authorises the collection of large amounts of information to regulate sex work. For instance, online sex work platforms have to log activity on their websites and provide it to the police on request. Moreover, potential employers have to ask for a permit, paving the way for a register of authorised employers. While the aim of ensuring that violent sexual offenders will never become employers is probably laudable, sex work gets its own classification number (NACE code), making sex workers officially registered and therefore traceable.[73] Nevertheless, it appears possible (and legal) to register under a different code, so as to limit the potential negative effects of this registration.[74]

The introduction of this new legal framework requires extreme caution. As some in the Federal Parliament propose to extend the HookUp system nationwide,[75] the principles of data minimisation must be imposed as a matter of urgency and the amount of data collected reduced. The separation of administrative files from police files must be guaranteed – especially if the security of the data cannot be ensured.

Indeed, in December 2022, the city of Antwerp suffered a significant cybersecurity breach when hackers infiltrated its systems. As a result, the city government had to temporarily go back to paper and pencil for its operations. The hackers obtained more than 500 gigabytes of data, including personal information, passports, id cards, financial documents and more.[76] It is unclear whether any data related to sex work was leaked, but the HookUp app has since ceased operations.[77] The hackers issued a ransom demand, warning that the data would be released unless payment was made. The hackers were not arrested and the data was not widely leaked, suggesting that the ransom may have been paid, although the mayor denies this.[78]

The Zwijndrecht police force, located in the province of Antwerp, was also subjected to a cyberattack in 2022. This resulted in the leakage of "car plates, crime report

71 *Ibid.*
72 UTSOPI, 2024. *Belgian labor law for sex workers: what and how?* URL: www.utsopi.be/our-work/decriminalisation/cadre-du-travail
73 Interview with the coordinator of an association supporting sex workers in Brussels, 04/08/2023.
74 According to a sex workers union representative who kindly provided feedback on this section.
75 Question n°1070 of 25/02/2022 by Ben Segers, a Flemish social-democrat, to the Minister of Justice. URL: www.lachambre.be/QRVA/pdf/55/55K0082.pdf
76 Michaël Temmerman. 'Site van hackerscollectief Play dat stad Antwerpen viseerde, plots offline gehaald'. *GVA*. 21/12/2022. URL: www.gva.be/cnt/dmf20221221_95447283
77 According to personal exchanges with a local social worker and with the civil servant in charge of sex work in Antwerp during the summer and autumn of 2023.
78 Belga. 'Bart De Wever affirme ne pas avoir payé de rançon après la cyberattaque ayant visé Anvers'. *RTBF*. 18/12/2022. URL: www.rtbf.be/article/bart-de-wever-affirme-ne-pas-avoir-paye-de-rancon-apres-la-cyberattaque-ayant-vise-anvers-11125227

files, investigation reports, and fines from the past 16 years".[79] These incidents highlight the vulnerability of data infrastructures and the risks associated with centralised data collection. It also calls for a re-evaluation of data management strategies, reinforcing that the best way to deal with sensitive information is to limit its collection.

b. Urban 'gangs' databases and profiling

In the early 2010s, violence and killings allegedly committed by so-called 'urban gangs' led to Belgian police making the policing of these groups a priority issue.[80] A central aspect of the police response included the creation of databases on these supposed 'gangs'. The databases listed information about alleged 'gang' members to assist with and facilitate monitoring, surveillance and targeting.

The conception of these groups both as 'urban' and as a 'gang' is entirely racialised. Racist stereotypes and fear-mongering proliferated. 'Gang' members were compared to 'child soldiers' and 'social' programs were developed to teach 'gang' members that "Belgium is not Africa" – even though the vast majority were born in Belgium or had grown up in Belgium.[81]

It is widely acknowledged that 'gang' narratives are underpinned by racist and classist ideologies, and used by police to target young people from minoritised ethnic backgrounds.[82] Individuals identified as part of these 'problematic groups' share a common profile: they are in a position of vulnerability and are victims of discrimination.[83]

Indeed, the parameters defining who is included on 'urban gangs' databases are extremely vague. As Rémy Farge, from the *Ligue des droits humains* (LDH), explains:

> "For the police, the much broader definition covers any group of people disrupting public order and security. It is this latter definition that is used as a tool for police investigation and information gathering".[84]

The question was put to the DPO of Charleroi police force. He acknowledged that information-gathering on 'gang' members is based on correlations rather than facts:

> "Strictly speaking, there is no formal definition; it is a question of offences that are recorded, regularly committed by the same people or on the same territory and that create a public order problem. The correlations thus established (facts and people, relations between people) are proposed to

79 Ionut Ilascu. 'Antwerp's city services down after hackers attack digital partner'. *Bleeping Computer*. 06/12/2022. URL: www.bleepingcomputer.com/news/security/antwerps-city-services-down-after-hackers-attack-digital-partner

80 GPI. *Plan national de sécurité 2012-2015 : Veiller ensemble à une société sûre et viable*. URL: www.police.be/5998/sites/5998/files/downloads/fr/Brochures%20informatives/PNS2012-2015.pdf

81 Mireille-Tsheusi Robert. '« Bandes Urbaines Africaines » : Un Produit Made in Belgium'. *Politique*, 01/06/2012. URL: www.revuepolitique.be/bandes-urbaines-africaines-un-produit-made-in-belgium

82 Patrick Williams and Eric Kind. 2019. Data-driven Policing: The Hardwiring of discriminatory policing practices across Europe. ENAR. . URL: raceandpolicing.issuelab.org/resources/36920/36920.pdf

83 Mireille-Tsheusi Robert. "« Bandes Urbaines Africaines » : Un Produit Made in Belgium". *Op. Cit.*

84 Rémy Farge, 2020. 'Police du futur et nouvelles technologies du profilage ethnique'. *La chronique des droits humains*. pp. 13-16.

> the magistrate of reference and the 'gang' is thus created. This is mainly a vernacular term".[85]

This vagueness surrounding inclusion in 'urban gangs' databases poses significant risks for discrimination on the basis of race and class. As Farge explains, police information-gathering about alleged 'gang' members will largely be informed by the racial biases of individual officers:

> "An analysis of the police reference database containing these urban gangs shows that the figures, location and census of these gangs 'must be put into perspective, depending on how police officers see them'.[86] The census also depends on the officer who reports the offence: 'This qualification therefore depends on chance, the perception of the police officer, the reporting by the latter or the recording in the database', while 'these figures are very often used by the media to show some kind of increase or to illustrate a news item.'
>
> Police statistics do not represent reality, but a recorded image of delinquency or crime, and are influenced by many factors. Their recording depends in part on the representations victims and institutions have of the criminal justice system: 'In this system of representations, certain individuals or groups present a particular vulnerability because, as a result of a complex ideological set-up, they embody at a given moment the feeling of a threat'[87]."[88]

The consequences for being registered as a 'gang' member can be serious. The DPO of the Charleroi police force wrote: "The fact that the photo is available allows the police officer, during a security patrol, to identify the person to be monitored, searched or stopped".[89]

'Urban gangs' databases serve the purpose of facilitating investigations, a policeman explains. The dehumanising language they use is indicative of the racism at play:

> "For example, someone snatches a bag from an old lady and she tells us that it is a gang of three or four Black people. She knows how to describe one of them. So we have one. Who are the other three? We do not know. We will check the computer, see the last thing this guy did and who he did it with. He may have been arrested other times with others. And so we are going to show pictures and like that, we are moving forward little by little".[90]

As pointed in a recent study on the discriminatory potential of the i-Police programme (considered in detail in section 3), the Belgian criminal justice system has been singled out on several occasions for its racist practices, particularly with regard to ethnic profiling.[91] The United Nations Committee on the Elimination of

85 DPO of Charleroi police force in his written answers to our survey. 02/03/2023.

86 L. Witvrouw, M. Born, F. Glowacz. 2015. 'Bandes urbaines et groupes délinquants en Belgique. Représentations et savoirs'. *Criminologie*, pp. 39–63.

87 I. Ravier *et. al.* 2016. 'Vers une image chiffrée de la délinquance enregistrée des jeunes en Région de Bruxelles-Capitale'. *Revue de Droit Pénal et de Criminologie*, no. 2, pp. 119-133.

88 Rémy Farge, 2020. 'Police du futur et nouvelles technologies du profilage ethnique'. *Op. Cit.*

89 DPO of Charleroi police force in his written answers to our survey. 02/03/2023.

90 Sylvia Bruier Desmeth, Valérie Caprasse, Jenneke Christiaens, Dominique De Fraene, Els Enhus, Carla Nagels, Sybille Smeets. 2012. *À la recherche des bandes urbaines : Discours des professionnels*. Bruxelles. SPP Intégration sociale ; Politique des Grandes Villes. URL : www.mi-is.be/sites/default/files/documents/etude_bandes_urbaines.pdf

91 Jérémiah Vervoort, 2021. *I-Police ou l'art de prédire la discrimination*. Travail de fin d'études. Brussels:

Racial Discrimination (CERD) warned in 2014 "that persons of foreign origin are overrepresented in the criminal justice system, including with respect to rate and length of incarceration".[92]

The Belgian branch of Amnesty International published a report on ethnic profiling in 2018.[93] The report concluded that half of police officers surveyed acknowledge the problem of ethnic profiling. While officers understand the need for legitimate grounds for all stops, ambiguous guidance has led to a broad interpretation of the law and increased reliance on intuition. However, Amnesty notes that this intuition is often associated with stereotypes.

The publication of Amnesty International's report led to public debates in the Federal Parliament.[94] However, the situation does not appear to have improved, as the 2021 CERD report states:

> "The Committee is concerned that racial profiling by the police remains a persistent problem in the State party [Belgium] and that there is no law explicitly prohibiting such profiling. The Committee is also concerned that there is a risk of abuse in practice based on the interpretation of the term "reasonable grounds" that is used in [...] the Police Functions Act, in connection with the powers of police officers to carry out identity checks. The Committee is further concerned about the lack of comprehensive data, disaggregated by ethnicity or national origin, on persons who are targeted by identity checks and victims of racial or ethnic profiling".[95]

A 2021 study provided further evidence of this problem. An ethnographic investigation undertaken in two Belgian police forces revealed that an individual's identification check was predominantly influenced by what police officers refer to as their "gut feeling", "sixth sense", or "radar". Police intervention against someone was found to be determined not only by their behaviour but also by personal characteristics, including gender, ethnicity, age, socio-economic status, and clothing. Moreover, "certain (groups of) individuals are associated with the image of 'troublemakers', which in the eyes of the intervening inspectors justifies a tougher approach".[96]

Police biases influence police action, resulting in certain groups facing increased stops, arrests and imprisonment. Under these circumstances, it is difficult to envisage how the Belgian criminal justice system can escape the criticism that big data policing reproduces discrimination.

Université libre de Bruxelles.

92 CERD. 2014. '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. URL: tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CERD%2FC%2FBEL%2FCO%2F16-19

93 Amnesty International Belgium. 2018. 'You Never Know With People Like You', URL: www.amnesty-international.be/sites/default/files/bijlagen/ethnic_profiling_executive_summary_en.pdf

94 Nawal Ben Hamou. 2019. 'Le profilage ethnique'. *Chambre des représentants de Belgique.* 54K3683001. URL: www.lachambre.be/FLWB/PDF/54/3683/54K3683001.pdf

95 CERD. 2021. 'Concluding observations on the combined twentieth to twenty-second periodic reports of Belgium'. *United Nations Committee on the Elimination of Racial Discrimination*. cerd/c/bel/co/20-22. URL: tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CERD%2FC%2FBEL%2FCO%2F20-22

96 Inès Saudelli. 2021. *Mag ik uw identiteitskaart zien? Een kwalitatief onderzoek naar identiteitscontroles uitgevoerd door de Belgische lokale politie*. PhD Dissertation. Vrije Universiteit Brussel.

c. Data discrimination in employment screenings and security clearances

Employees in Belgium can be subjected to security screening by their employer or other authorities. These screenings can take place in a variety of circumstances. They may be required for particular job assignments or duties, or to allow certain privileges that are contingent on an employer's review of one's loyalty, integrity, discretion, and overall 'good character'.

These screenings includes searches of police, security and administrative databases, and can be a prerequisite for:

- obtaining the 'security clearance' needed to access classified information;
- authorisation to perform certain duties during diplomatic events, such as EU government summits;
- temporary access to sensitive areas, such as within nuclear infrastructures;
- obtaining an airport badge or working in/with the military.[97]

A wide range of databases can be accessed for security screening, including:

- the Schengen Information System (SIS, an EU police, judicial and immigration database);
- the BNG-ANG (see above);
- common databases (see above);
- judicial databases;
- Limosa (the register of foreign workers);
- a database on illegal employment and social security fraud;
- and the special operational police database developed and managed by the 'Central Directorate for Combating Serious and Organised Crime Linked to Terrorism, Radicalism and Extremism'.[98]

In an interview with the COC, we asked what types of information this may include:

> "Everything. Judicial information, hard information and also soft (administrative or judicial) police information. There can be reports that you were a suspect of [committing] a theft, but that you were never convicted, or you accepted a transaction [a plea bargain] from the Public Prosecutor's Office, etc. That information will be used to give or not give a clearance".[99]

97 Appeal Body for security clearances, certificates or advice. URL: beroepsorgaan.be
98 Arrêté royal du 8 mai 2018 déterminant la liste des données et informations qui peuvent être consultées dans le cadre de l'exécution d'une vérification de sécurité. URL: beroepsorgaan.be/images/boor/6_1/Veiligheids_verificaties_gegevens.pdf
99 Interview with Frank Schuermans (COC), 17/02/2023.

The website of the appeal body states:

> "Not only can the authorities consult existing records, but they can also conduct further inquiries (with neighbours, employers, etc.). The applicant's spouse and other adult household members may also be subject to investigation".[100]

In Belgium, these checks are mandatory for people working at ports, airports, or nuclear plants,[101] but are gradually becoming more common. Even workers at large music festivals, for instance, have undergone screenings, as will be discussed below. There are numerous examples of people being barred from employment because of information held about them on police databases.

For example, in 2023, it was announced that port workers in Antwerp port would be subjected to vetting procedures as part of a crackdown on drug trafficking. Though it remains unknown which databases will be accessed as part of these procedures, it is likely this will include information on police databases. In February 2023, the Prime Minister's official website stated:

> "The screening of port staff has started. It involves some 16,000 people in sensitive posts within the port who will be screened by security and intelligence services for links to organised crime. This process has started in recent weeks. The various port companies designated security officers who will act as liaison officers. They are currently undergoing a thorough vetting by State Security. After that, they can transfer the details of personnel to be screened within their companies".[102]

This scenario presents a significant challenge to the equitable rights of citizens, especially when screenings become obligatory for accessing a growing range of services and opportunities. Employer access to police databases, although indirect, also holds serious potential for discrimination. This is illustrated well by the following testimony, in which a young man was barred from a job at a local youth club because of information held about him on a police database:

> "I am a 22-year-old man. Three years ago, I was a victim of a stabbing. Out of nowhere I was stabbed. It was not just a physical blow, but it was a serious mental blow. To overcome it, I benefited a lot from my youth work. I have been going there for around 8 years. In the past few years I have gotten involved in a project where you are deployed to events in the area to work as a steward. I love doing it and I get a lot of responsibility. I find it very important to make sure people feel safe because I myself have felt so unsafe. [...]
>
> For four years, I have been doing voluntary work as a steward at a youth club in the city. This summer I applied for a role to be in charge. I got an email to say I was accepted. But the day before I was going to sign my contract, the coordinator told me I could not start. I had not passed the screening. He referred me to a local police officer, but he could not tell me what had come out as negative in my screening.

100 Appeal Body for security clearances, certificates or advice. URL: beroepsorgaan.be
101 Interview with Frank Schuermans (COC), 17/02/2023.
102 'Nationale drugscommissaris en meer politie in Antwerpse haven in strijd tegen drugsmaffia'. 16/02/2023. URL: premier.be/nl/nationale-drugscommissaris-en-meer-politie-antwerpse-haven-strijd-tegen-drugsmaffia

> When my youth worker approached his contacts at the police, they said that a screening had not happened. The irony was that I could still work as a steward in the youth club. I kept doing it because I enjoy doing it so much and all my friends also come to the youth club.
>
> I never received anything on paper. I have never had a criminal record and I have never been contacted by the police. Except for once, a long time ago, when I was a minor. I was out in the neighbourhood with my brother to go and do the shopping. At the same time, there was a forbidden demonstration taking place, from an 'extremist' Islamic organisation. We were surrounded by the police. My brother was allowed to return home because he was working as a journalist at the time and could show them his press card. I was taken to the police office and I needed to go to a municipal administrative sanctions officer. He assigned me community service.
>
> I never meant to take part in the demonstrations. I was just in the wrong place at the wrong time. The municipal administrative sanctions officer told me then that it would definitely be removed from my criminal record. I think that I am still somewhere in the database though and that is why I did not make it through the screening. Even when I catch a flight, they take me out the queue for an inspection and they tell me that I am blacklisted.
>
> In September, I am planning on registering for a security training. I am scared I will not make it through the screening for that either. It is still my dream to work in the security sector.
>
> This whole situation really upsets me. I find that society is ungrateful. I have done my best for young people and youth work. I have done so much volunteer work for the city. Being linked to terrorism hurts".[103]

This testimony highlights the severe consequences that arise from racist and Islamophobic prejudices within the police, and reflected in police databases. The young man was falsely registered in a police database linking him to terrorism because of his skin colour and because he was Muslim or perceived to be Muslim. His experiences also reveal the persistence of such data in police databases. Years after the events took place, the information stored about him still leads to questioning and inspection at airports, and affects his chances of employment. The story emphasises the severe harms that police databases pose by reinforcing existing discrimination and injustice.

D. 'Counter-terrorism' data screenings

In addition to the screening conducted for security clearances, the police also undertake certain preventive and automated analyses. There is limited information available on this subject. However, in 2018, a Federal Police spokesperson declared:

> "Our police and intelligence services already use software such as Radix and Vera 2 to assess risks and threats in the fight against terrorism. This involves weighing parameters and suspect names against each other to set priorities. Our services use the same parameters as other countries, albeit adapted to the national context and with different names for the tools, such

103 Quoted in Nina Henkens and Ikrame Kastit. *Looking at the deradicalisation policy from a different perspective*. Uit de Marge. 2019. URL: uitdemarge.be/wp-content/uploads/2019/11/ENG_Looking-at-the-deradicalisation-policy-from-a-different-perspective.pdf

as Kim in the Netherlands and RADAR-iTE in Germany".[104]

These issues came to the fore following the November 2015 Paris attacks and March 2016 Brussels bombings. Anti-radicalisation measures were implemented in Belgium under the pretext of safeguarding national security, and have had significant impacts on individuals. Nadia Fadil, a sociology professor at KU Leuven, coordinated a study on the effects of counter-terrorism procedures on Muslims in Belgium. These consequences include negative security assessments, obstacles accessing financial services, border refusals, repeated police raids and excessive police checks.

The constant excessive checks constitute a form of ongoing surveillance and harassment that not only disrupts the personal lives of those targeted, but also infringes on their civil liberties. Such practices not only violate personal freedoms and privacy but also create an atmosphere of fear and mistrust.[105]

In many cases, the initial trigger for police suspicion was if an individual had acquaintances, friends, or family members who had gone to Syria and were suspected of involvement with Daesh (also known as the Islamic State). This approach of guilt-by-association has unfairly ensnared individuals who may not have had any involvement themselves.

Furthermore, an individual's participation in associations, particularly those advocating for social justice or critical viewpoints, has been a basis for targeting individuals. This conflates dissent with 'extremism', undermining the fundamental right to freedom of association.[106] In addition, Committee T (the independent Committee for Vigilance in the Fight against Terrorism) consulted law firms that had appealed denials of security clearances. They emphasised that among those targeted there was an "over-representation of Belgo-Moroccans or people of North African origin, particularly when it comes to airport workers".[107]

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 exacerbates their susceptibility to harm and marginalisation.[108]

A separate report by Nadia Fadil and other scholars indicates that the concept of 'radicalisation' itself merits scrutiny. Professionals within the field of prevention are sceptical of the term and its application, suggesting a need for re-evaluation:

> "Most of the stakeholders interviewed disapprove of the discussion of radicalisation. They assert that this conversation adds to the stereotyping of the youth and challenge the belief that radicalisation is a hazard or

104 Lars Bové. 'Politie gaat criminaliteit via data voorspellen'. *De Tijd*. 30/08/2018. URL: tijd.be/politiek-economie/belgie/federaal/politie-gaat-criminaliteit-via-data-voorspellen/10044356.html
105 Nadia Fadil, Arthemis Snijders, Kaoutar Boustani Dahan, Lore Janssens. 2022. Entre droits fondamentaux et surveillance: Les effets secondaires de la lutte contre la radicalisation sur les musulmans belges. Rapport de recherche. *KU Leuven*. ISBN: 9789071047244.
106 *Ibid.*
107 Comité T. Rapport 2021. *Op. Cit.*. p. 41.
108 Fadil *et al.*, 2022, Entre droits fondamentaux et surveillance, *Op. Cit.*

> concern. Some defend the privilege of young people to rebel against society, to demand their entitlements or to highlight issues, without automatically interpreting it as hazardous. Professionals also question the premature identification of radicalisation. They express concerns regarding the suitability and feasibility of such detection: not only can it erode the trust relationship, but they also propose that the profile is ambiguous and relies on stereotypes or caricatures. Furthermore, they perceive assessment to be a challenging, if not insurmountable, undertaking".[109]

There is a significant risk that these issues will become more prevalent in the future. Local authorities are due to implement a new approach, in which they will take police records into consideration when deciding to reject, suspend, or revoke licenses for establishments and businesses, or to close them down.[110]

Moreover, the efficacy of such widespread monitoring is debatable. Security services have been screening the data of people travelling by air for years and have processed dozens of millions of passenger records. A report from the COC points to all sorts of problems with this approach, questioning whether this "huge invasion of our privacy" is effective in the fight against terrorism and organised crime.[111] It is also illegal under the case law of the European Court of Justice and the Belgian Constitutional Court.[112]

Finally, these screenings, designed to ensure security and suitability, draw upon a vast amount of information. However, concerns arise regarding the veracity of these information sources. Some files are generated for intelligence purposes and may contain unfounded and unevidenced implications, conjectures, and inferences. The pivotal issue is the origin of these potentially unreliable sources, which frequently stem from law enforcement or intelligence agencies. This creates a conundrum. Individuals lack direct access to these sources, impeding their ability to rectify erroneous information.

109 Lore Janssens, Nadia Fadil & Maryam Kolly. 2022. 'Entre secret et partage de l'information: La négociation du secret professionnel et le partage d'information dans la lutte contre la radicalisation violente'. Rapport de recherche. *KU Leuven*. ISBN: 9789071047220. PP 29-30.

110 Projet de loi relatif à l'approche administrative communale, à la mise en place d'une enquête d'intégrité communale et portant création d'une Direction chargée de l'Évaluation de l'Intégrité pour les Pouvoirs publics. URL: lachambre.be/kvvcr/showpage.cfm?section=/flwb&language=fr&cfm=/site/wwwcfm/flwb/flwbn.cfm?lang=F&legislat=55&dossierID=3152

111 Lars Bové. 'Waakhond betwijfelt of screening vliegtuigpassagiers doeltreffend is'. *De Tijd*. 28/12/2022. URL: tijd.be/politiek-economie/belgie/algemeen/waakhond-betwijfelt-of-screening-vliegtuigpassagiers-doeltreffend-is/10437318.html

112 La loi belge PNR « Passenger Name Record » recadrée par la Cour de justice de l'Union européenne. *Ligue des droits humains.* URL: www.liguedh.be/la-loi-belge-pnr-passenger-name-record-recadree-par-la-cour-de-justice-de-lunion-europeenne

e. Challenging the indirect right of access

The right of access to police data is enshrined in Article 14 of the EU's 'Law Enforcement Directive' – the equivalent of the GDPR for law enforcement agencies.[113] Article 14 states that people should have the right "to obtain from the [data] controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data", as well as a set of information on such data. This right of access enables citizens to exercise their rights to erasure and rectification.[114]

The right of access is, in principle, direct. However, Belgium utilises indirect access to data processed for police purposes, differing from most European countries. This means that access requests are submitted to the COC instead of the data controller or processor. Article 42 of the Belgian Data Protection Act (DPA) states that the COC shall only provide the requester with information that "the required checks have been conducted".[115] There is no legal right to see the data itself. Such limitations on access are so severe that they effectively nullify the right of access itself.

This problematic situation was brought before the European Court of Justice (ECJ). The case was initiated by an individual who was denied employment at a music festival when they failed the security screening. Lawyer Catherine Forget, in partnership with the *Ligue des droits humains* (LDH), represented the claimant and secured a landmark victory at the ECJ. It eventually transpired that the denial resulted from information held about the claimant's past attendance at ten demonstrations (without being subject to any legal arrest).

The claimant utilised his right of access through the COC, who responded that "all checks have been carried out". As a result, the claimant was unable to be aware of, and much less object to the charges against him. Additionally, it remains unclear why his exercise of a fundamental right – the right to demonstrate – was documented in a police database.

The ECJ ruled that this form of indirect access to police databases contravenes EU law.[116] The indirect exercise of one's rights was originally intended as an additional safeguard, allowing the exercise of rights when limitations apply. Making it the only form of redress available fundamentally undermines the right of access. Consequently, the Belgian state will have to change the law to rectify this predicament.

113 'Law Enforcement Directive'. *EUR-Lex*. 27/04/2016. URL: data.europa.eu/eli/dir/2016/680/oj

114 Art. 16 of Directive 2016/680. URL: eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A32016L0680

115 Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. URL: etaamb.openjustice.be/fr/loi-du-30-juillet-2018_n2018040581.html

116 ECJ . Case C333/22. Judgement of the Court (Fifth Chamber). *Curia. 16/11/2023.* URL: curia.europa.eu/juris/document/document.jsf?text=&docid=279747&cid=12850052

3. The future of Belgian police databases

After the COC published a highly critical report on the management of police databases,[117] the COC was invited to the Federal Parliament to discuss the issue. On this occasion, its chair Frank Schuermans presented their main conclusions:

- the police IT systems date back to "prehistorical" times, and require a huge amount of work to maintain;
- there is a lack of standardisation, a lack of clear guidelines. The differences in information management between police forces are therefore very important. Some departments and police forces attach great importance to it while for others, everything remains to be done;
- training in police academies is inadequate. There is no curriculum, no syllabus on data protection. Hence new recruits are poorly trained on these issues;
- there is a lack of expertise among those in charge. There are still local police forces where there is no DPO or where the DPO has another role, such as DPO and director of operations or IT manager at the same time, which creates a conflict of interest.[118]

As demonstrated above, racialised and marginalised groups and individuals face discrimination and increased criminal justice and other punitive outcomes because of the data held in police databases. This is particularly the case in the context of policing 'gangs' and counterterrorism procedures. There were discussions in the Federal Parliament on ethnic profiling by the police,[119] following Amnesty's critical 2018 report.[120] However, at present, there is insufficient political drive to address the challenges of managing databases and the discriminatory consequences of data-driven policing for those who are most marginalised.

117 COC, 2023. DIO23001. *Op. Cit.*
118 Hearing of the COC at the Federal Parliament following his report on the BNG-ANG. 28/06/2023. *Chambre des représentants de Belgique*. Doc 55 3467/001.
119 Nawal Ben Hamou. 2019. 'Le profilage ethnique'. *Chambre des représentants de Belgique.* 54K3683001. URL: www.lachambre.be/FLWB/PDF/54/3683/54K3683001.pdf
120 Amnesty International. 2018. Belgique : Le profilage ethnique, injuste et inefficace. URL: www.amnesty.be/infos/actualites/article/belgique-profilage-ethnique-injuste-inefficace

III. The federal 'i-Police' project

The i-Police project is a central focus of this report on 'predictive' and data-based policing. The federal project has significant funding and multiple implications for civil liberties and human rights.

The General Commissioner of the Federal Police, in an official announcement from the Ministry of Interior, said:

> "i-Police will make the Belgian police force one of the most advanced in Europe in terms of data governance. The system will analyse information, make it automatically available to police forces, suggest investigations and provide numerous time-saving tools, such as automatic translations. i-Police will enable us to pave the way for a future-oriented Integrated Police at the service of citizens".[121]

The same announcement reads:

> "i-Police 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. [...] In addition, the system offers citizens a guarantee of confidentiality and transparent control. Police officers will have limited and controlled access to citizens' information, based on their function and mission at the time".[122]

The first mention of the i-Police project that we have been able to find dates back to the Minister of Interior's General Policy Note of 2013. The Note stated that the i-Police project aimed to harmonise the Federal Police (FEEDIS) and local police (ISLP) IT systems, as both were – and still are – outdated and costly to maintain.[123] ISLP was developed in the early 1990s and FEEDIS in the early 2000s.[124]

A feasibility study for the i-Police project was conducted in 2014 and increased the scope of the project. The Minister of Interior's 2015 Policy Note stated:

> "The aim is to use sensor networks to intelligently integrate information collected at local and federal level with current closed and open (authentic) sources, and then to make the best use of this information by processing it using intelligent automated tools. Equipping the police with 'next generation' technology within the police chain will enable intelligent policing, *i.e.* a community-oriented, problem-solving and information-driven fusion of police functions".[125]

121 Annelies Verlinden. *i-Police: l'avenir de la police est numérique*. 07/05/2022. URL: verlinden.belgium.be/fr/i-Police

122 *Ibid.*

123 Joëlle Milquet. *Note de politique générale – Police fédérale et fonctionnement intégré*. Chambre des représentants de Belgique. 06/11/2013. 53K3096012. URL: www.lachambre.be/FLWB/pdf/53/3096/53K3096012.pdf

124 GPI. 2020. *i-Police tender. Appendix H – Context and scope of the tender*.

125 Jan Jambon. *Note de politique générale – Police fédérale et fonctionnement intégré*. Chambre des représentants de Belgique. 04/11/2015. 54K1428004. URL: www.lachambre.be/FLWB/PDF/54/1428/54K1428004.pdf

In 2016, the Belgian federal government allocated funds to establish the i-Police system and centralise all police data within cloud infrastructure. The system's operational launch was set for 2020 and would be the result of a collaboration between the Ministry of Interior, the Digital Agenda, and the Ministry of Justice.[126] The National Security Plan 2016-2019 said:

> "In the area of intelligent policing, the Federal Police is working on an innovative new solution ('i-police'), which will replace the current mainframe with new, modern technologies. These new technologies should enable information to be better 'linked', exchanged and analysed, and this quickly. The police must be able to work and act on the basis of an integrated analysis of structured and unstructured information available both internally and externally".[127]

In September 2018, the federal and local police issued a joint press release outlining plans for 'predictive' policing as part of i-Police.[128] They envisaged 'predictive' policing experiments in Antwerp and other local police forces following the council elections of 14 October 2018. Data would be sourced from police databases, including the frequency of specific crimes in particular areas. External data sources were deemed equally significant.[129]

Figure 8. The i-Police logo[130]
Source: *Rapport annuel 2022 de la Police Fédérale*, p. 82.

126 Rosamunde Van Brakel. *Automating Society 2019: Belgium*. *Op. Cit.*
127 GPI. *Plan national de sécurité 2016-2019 : Aller ensemble à l'essentiel*. p. 86. URL: www.police.be/5998/sites/5998/files/downloads/PNS2016-2019.pdf
128 Kathleen Heylen. 'Politie wil in de toekomst criminele feiten "voorspellen" via algoritmes'. *VRT news*. 30/08/2018. URL: www.vrt.be/vrtnws/nl/2018/08/30/politie-wil-criminele-feiten-kunnen-voorspellen-aan-de-hand-van
129 Rosamunde van Brakel. *Automating Society 2019: Belgium*. *Op. Cit.*
130 According to a Senior Advisor R&D and ICT Strategy Belgian Federal Judicial Police, the central orange line symbolises the collection of data; the light blue line the creation of value from it; while the whole process is protected by the thick dark blue shield.

In 2021, the Federal Police published the contract award notice[131] for the project. French IT and consultancy company Sopra Steria[132] would receive €300 million over seven years (2021-27). It would take four years to build the system, after which the contract covered three years' of maintenance.[133]

The tender for the project included a fictional scenario depicting a day in the life of 'John', a policeman in a fictional police force. The intention to develop 'i-Police' into a 'predictive' policing programme is clear:

> "A 'pop-up' window appears [...] to say that an 'anomaly' was observed. The police application has noted that a high number of bicycle thefts have been registered around a certain location and around certain times. The system can recognize this because our "data scientists" in Brussels have programmed the system to recognize these 'anomalies'. [...] The system indicates that recently some suspicious transactions were reported at that site. [The superintendent] plans a regular patrol via the e-briefing tool for patrol officers"[134]

Elsewhere, the tender discusses a 'preventive' plan for the police district:

> "Through computerized analysis of a number of recent incidents, traffic accidents, and the plans for opening of a new SME [small and medium-sized enterprise] Zone, a "predictive" model will be designed and a plan for preventive monitoring of the SME buildings will be developed".[135]

Further on, the tender envisages another type of 'predictive' application:

> "The Patrol department, the management of Operations and some neighbouring police zones jointly plan a large-scale police action on Friday night. The objective is to perform an extensive control in bars and nightclubs since there was a reported increase in the number of knife-related crimes on Friday in the last few months".[136]

The system also allows for heightened surveillance of 'suspicious' individuals:

> "At the end of the day, John receives a call from a Brussels-based investigator. The text message that John dictated during a residence check, showed that another person was present in that house. This person is being monitored as part of a terrorism investigation. The colleague from Brussels – who subscribed to a 'digital subscription' with regard to the person John has encountered – has thus received an automatic 'alert' that a police officer in a zone happened to come across this person in the course of a routine residency check. This triggered him to contact John directly to ask for additional information".[137]

131 'i-Police tender'. *Tenders electronic daily*. 2021. URL: ted.europa.eu/udl?uri=TED:NOTICE:675394-2021:TEXT:FR:HTML&src=0&tabId=4
132 Sopra Steria company. URL: www.soprasteria.be
133 Minister Verlinden's answer to question 1323 by Yngvild Ingels, a Flemish Nationalist member of the Federal Parliament. 14/07/2022. URL: www.lachambre.be/kvvcr/showpage.cfm?section=qrva&language=-fr&cfm=qrvaXml.cfm?legislat=55&dossierID=55-B089-1192-1323-2021202215762.xml
134 GPI. 2020. *i-Police tender. Appendix H – Context and scope of the tender*. p. 35.
135 *Ibid*, p. 35.
136 *Ibid*, p. 36.
137 *Ibid*, p. 35.

1. i-Police data

Belgian police database will feed the future i-Police programme, along with many other data sources. The i-Police tender includes a fictional scenario following an ID check:

> "Their system automatically controls 10 different databases (National Register, national police databases and foreign police databases, prisons, foreign fighters ...) and warns immediately whenever there is a hit on any of the controlled identities".[138]

The police are planning to include a vast range of data sources in i-Police, as shown in the figure below.

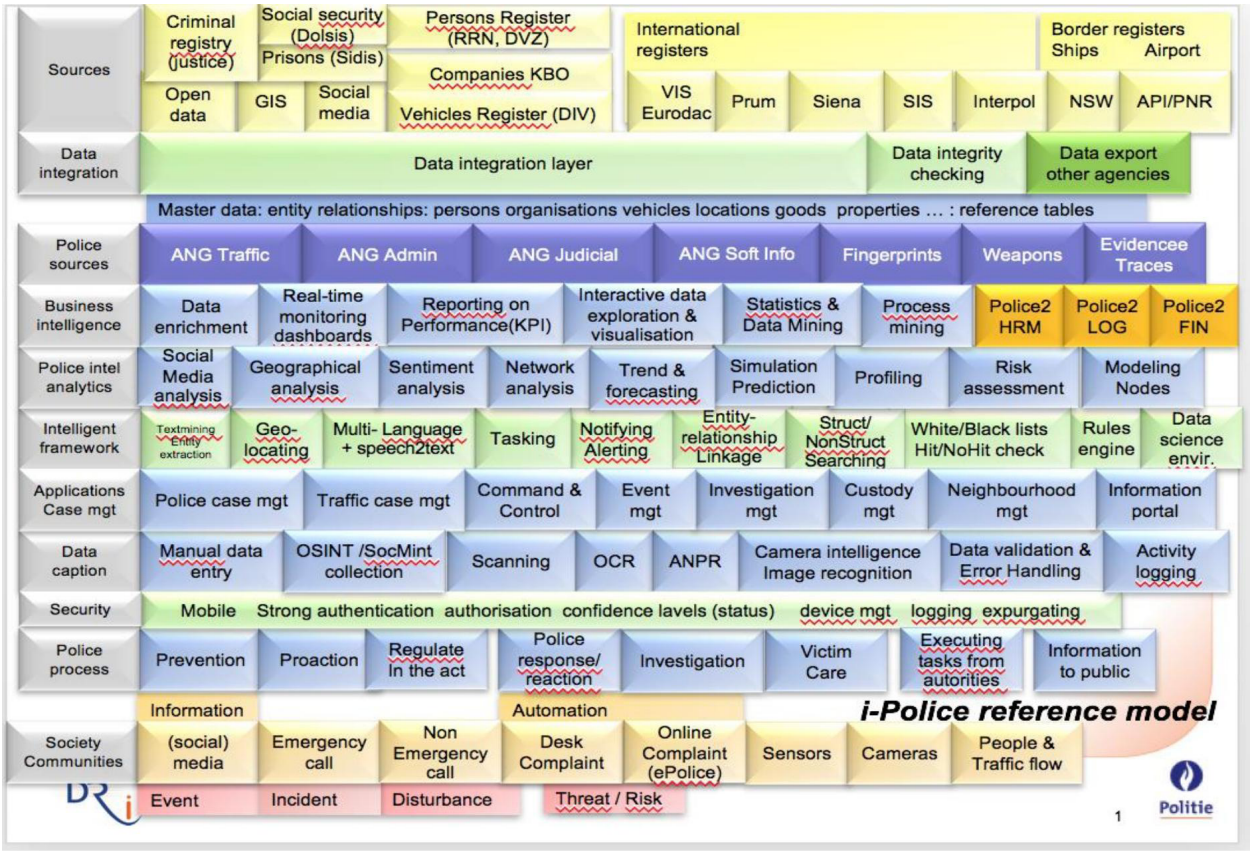

Figure 9. Future "business architecture" of the i-Police project
Source: i-Police tender. Appendix H. p. 58.

Both the extent and types of data provide cause for concern. Data from various databases will be brought together in a 'data lake': a repository that uses multiple sources, while keeping them in their original format.

Furthermore, police databases usually differentiate between 'validated' and 'non-validated' information. 'Validated' information has been verified, while 'non-validated' information is unverified. The Chair of the COC has expressed concern over the combination of verified and unverified information in the i-Police 'data lake' :

138 *Ibid*, p. 36.

> "There is also a lot of non-validated information. [...] That difference between validated and non-validated information is going, I fear, to disappear in a system of data lake in the new concept of i-Police. So the average police officer [...] will have access to much more information and much more non-validated information, which of course is a huge worry, and not only for the person itself (the alleged suspect), it is a huge worry for the judicial system as a whole. It is a huge worry for everybody. [...] But that's clearly the way that the police but also politics and the ministers [...] want to go: give every police officer as much information as he needs at any time [...]. It's very possible in our system [...] [that] you have been acquitted by court, but you're still in the database. And when you encounter a police officer, he then could confront you with those data on which you were actually acquitted by court. And so that's a huge issue".[139]

The chair of the COC has extensive experience as a criminologist and as a former member of Committee P. We asked him for his opinion about the evolution of the use of information in the police:

> "I often talk about the 'disintegrated police' because in reality, even in the management of police information, which should be amongst the first areas of integration, we are still not there. Fortunately, the BNG-ANG is centralised, but even at that level there are big differences in the way people work, in the way they encode data, in the way they use the BNG-ANG, and so on: the level of expertise is very low. So if you ask me what I think about the future of information management, I have to say that I am relatively pessimistic. For instance, the 'information crossroads'[140] are services that should be integrating police information. In practice, if you want to get rid of a police agent, that is often where you put them. That says a lot, doesn't it?"[141]

The i-Police 'data lake' appears to prioritise quantity over quality. This approach is concerning as it lacks consideration for the accuracy and reliability of the data, while the implications can be extremely serious. In their ambition to collect as much data as possible, disregarding for the principle of data minimisation, the i-Police vision could be summarised as: "Take them all; let the algorithm sort them out".

139 Interview with Frank Schuermans (COC), 17/02/2023.

140 *Carrefours d'information d'arrondissement (CIA) – informatiekruispunten (AIK's)* provide a link between the federal and local levels for the operational exchange of administrative and judicial police information, according to the presentation of the integrated police. URL: www.police.be/5998/fr/a-propos/police-integree/presentation

141 Second interview with Frank Schuermans (COC), 11/10/2023.

2. Video surveillance

The i-Police project plans to integrate video surveillance footage and imagery. Here we examine the different types of image analysis software, such as facial recognition, already in use by Belgian police forces.

One type is live detection software. The Belgian police use this to receive alerts when potentially 'suspicious' activities are caught on camera and noticed by an algorithm. Relevant activities include: smoke, graffiti, littering, people running or loitering near a car, and other similar events. In practice, the software identifies numerous 'problematic' events over large areas with high false positive rates, ultimately leading operators to disregard the alerts. Despite this, the system could inadvertently impact privacy and lead to biased perceptions of events, shaped by technical capacities and it engineers' representations rather than democratic debate.[142]

Belgian police also use the BriefCam software,[143] produced by an Israeli company, for retrospective image analysis in investigations.[144] This software produces video synopses. It examines hours of camera footage and then categorises incidents according to certain criteria, such as the suspect's belongings, clothing colour or gender. This feature raises questions about potential unlawfulness. The Belgian legal framework on non-discrimination allows for targeted research based on objective criteria, which may include sensitive physical characteristics such as gender, but forbids the mass sorting of individuals on the basis of such criteria.

BriefCam is used by local police forces as well as the Federal Judicial Police. It is unique in that it incorporates face recognition surveillance technology. Local police forces tend to deny using this feature.[145] The Federal Police, for their part, make no secret of their use of face recognition surveillance: the tender they published for renewing their BriefCam licences mentions it.[146] There is however no explicit legal framework for facial recognition in Belgium.[147]

The use of face recognition surveillance has garnered attention by the Belgian press in recent years. In 2017, the Federal Police initiated a pilot project at Brussels airport to test the technology.[148] However, the system produced a significant

142 Sarah Brayne. 2020. *Predict and Surveil: Data, Discretion, and the Future of Policing. New York: Oxford University Press.*

143 BriefCam company. URL: www.briefcam.com

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

145 'Kortrijkse politie is één stap verwijderd van gezichtsherkenning'. *Datapanik*. 24/05/2019. URL: www.datapanik.org/2019/05/24/kortrijkse-politie-is-een-stap-verwijderd-van-gezichtsherkenning
We also asked a police force that uses BriefCam in Brussels and in broad terms, they provided the same answer.

146 Cahier spécial des charges n° procurement 2024 R3 005 relatif à la maintenance de la solution d'analyse d'images de vidéo surveillance « Briefcam » au profit de la Police Judiciaire Fédérale, p. 37. URL: enot.publicprocurement.be/enot-war/preViewNotice.do?noticeId=491396

147 The 'Arizona' government agreement does, however, envisage legalising facial recognition, see *Government statement*, 04/02/2025, p. 145. URL: www.lachambre.be/flwb/pdf/56/0020/56K0020001.pdf

148 Rosamunde van Brakel. 2021. 'How to Watch the Watchers? Democratic Oversight of Algorithmic Police Surveillance in Belgium'. *Surveillance & Society*, vol. 19, no. 2, pp. 228-240. URL: ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/14325/9779

number of false positives during testing, leading to its suspension. Despite this, a later visit by the COC revealed that the system remained partially operational, outside of any legal framework. Following the COC investigation, the project was ultimately banned.[149]

Later, concerns arose about the use of a Clearview AI system for face recognition surveillance. Clearview is renowned for retrieving huge numbers of photos from public data sources, such as social networks. In August 2021, a news site reported that the Federal Police had carried out searches using the Clearview application.[150] The police initially denied their use of Clearview, but the COC carried out an investigation that proved otherwise. It was then revealed that Clearview's pilot license had been provided at an event coordinated by Europol.[151]

These video surveillance developments raise serious concerns. They show that the Federal Police's use of technology lacks transparency, meaning that any potential illegalities are more likely to go undetected. Not only that, but the Federal Police have even lied to the supervisory authorities when their usage of video surveillance systems was revealed.

Given the examples of video surveillance software already used by Belgian police, the prospect of i-Police incorporating behaviour, facial and number plate recognition software suggests a panopticon of the most dystopian kind. It is essential to halt such an unbridled expansion of video surveillance. The *Ligue des droits humains* (LDH), along with several other local associations, support this stance. They are actively campaigning for a ban on face recognition, promoting the #ProtectMyFace hashtag.

Figure 10. #ProtectMyFace Campaign.
Sign the petition to ban the use of facial recognition technology in public spaces in Brussels.

149 COC, 2019. Rapport sur l'utilisation de la reconnaissance faciale l'aéroport national de Zaventem. *Organe de contrôle de l'information policière*. DIO19005. URL: www.organedecontrole.be/files/DIO19005_Contr%C3%B4le_LPABRUNAT_Reconnaissance_Faciale_Publique_F.PDF

150 Ryan Mac, Caroline Haskins and Antonio Pequeño IV. 'Clearview AI Offered Free Facial Recognition Trials To Police All Around The World'. *BuzzFeed News*. 25/08/2021. URL: www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table

151 COC, 2022. 'Rapport relatif à l'utilisation de l'application Clearview AI par la police intégrée'. *Organe de contrôle de l'information policière*. DIO21006. URL: www.organedecontrole.be/files/DIO21006_Rapport_Contr%C3%B4le_Clearview_F_00050441.pdf

3. Open-Source Intelligence (OSINT), algorithmic analysis and subcontractors

In addition to their own databases and video surveillance footage, the police aim to integrate external data sources into i-Police. This desire has been repeatedly expressed by local police authorities, the Federal Police, and criminologists engaged in the advancement of 'predictive' policing techniques. For instance, the i-Police tender cites as potential sources:

- "third-party data captured and managed by third parties (external sources). This category includes information that is immediately available to the police (for example, information from the National Register, Crossroads Bank for Enterprises, Vehicle Licensing Authority...) as well as information that can be legally obtained from third parties (*e.g.* antenna data from telecom operators);

- open data is data that is freely accessible to all and that can be used immediately. Falling under this category: (freely available) information from social media, information from the press".[152]

An open-source intelligence (OSINT) unit was established in April 2023 in Brussels. At the time of its creation, the office employed nearly ten staff members, and was expected to double in size by 2024. The unit relies on tools from the German company Maltego Technologies[153] and from Social Links,[154] which originated in Russia before moving to Western Europe and the US after the Russian invasion of Ukraine in 2022.

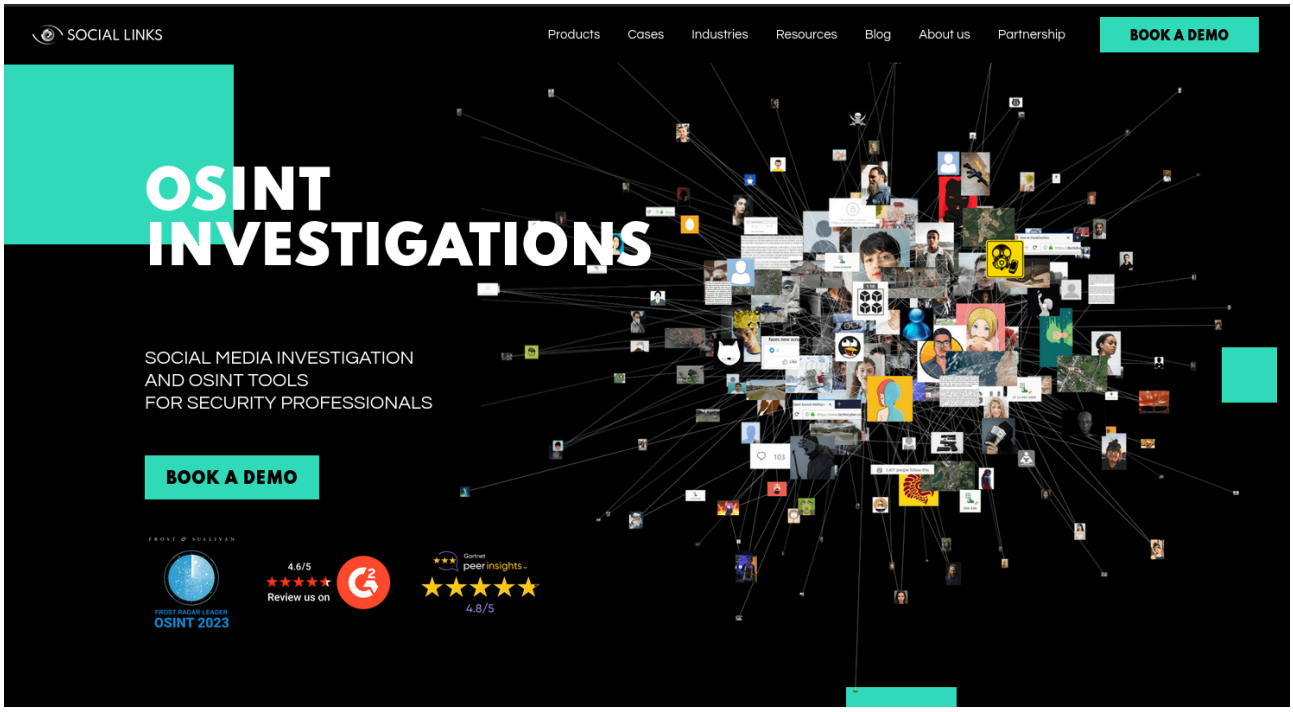

Figure 11. Home page of the Russian company Social Links website showing a social graph, 27/10/2023.

152 GPI. 2020. *i-Police tender. Appendix H – Context and scope of the tender*. pp. 43-44.
153 Maltego Technologies. URL: www.maltego.com
154 Social Links company. URL: sociallinks.io

As part of i-Police, the Federal Police OSINT division is preparing to implement the IntSight investigation and mass data analysis platform. This is produced by TA9, an Israeli technology company.[155] TA9 is part of the Rayzone group, run by Yohai Bar-Zakai,[156] who formerly served as Deputy Director of Unit 8200.[157]

Unit 8200 is "the Israeli Intelligence Corps unit of the Israel Defense Forces responsible for clandestine operation, collecting signal intelligence and code decryption, counter-intelligence, cyberwarfare, military intelligence, and surveillance".[158] Unit 8200 is responsible for developing 'Gospel', an AI system for generating Israeli Air Force bombing targets in Gaza, at a significantly increased rate than manually-generated targets.[159] It is believed that 'Gospel' has contributed to the intense bombardment of Gaza and killing of Palestinians in the latest escalation of Israeli violence and destruction.[160]

It is difficult to determine precisely which other companies and software will be integrated as part of i-Police's OSINT solutions. It is clear that Sopra Steria assumes the role of the main contractor for i-Police, with the support of consultancy company KPMG. According to a press report, they will collaborate with a diverse array of subcontractors, including companies such as Microsoft, the Canadian company NicheRMS365,[161] and the Israeli companies Interionet[162] and TA9/Rayzone.[163] A senior policy advisor in charge of ict strategy for the Belgian police assured us that all third-party entities will need to make necessary adjustments to ensure the compatibility of their software with Belgian legal frameworks.[164]

Another subcontractor for i-Police, Interionet, is headed by Yair Pecht, the ex-CEO of the Israeli cyberoffensive specialist nso Group. NSO is the company infamous for producing the Pegasus spyware, which has been used against multiple journalists, politicians and political activists. Intelligence gleaned through Pegasus has been linked to dire consequences, including the assassination of dissidents. nso's contentious track record, marked by deals with authoritarian regimes, has drawn international scrutiny. This has led its executives to multiply the number of satellite start-ups, such as Interionet.[165]

155 TA9 company. URL: www.t-a9.com
156 Rayzone Group. URL: rayzone.com
157 'A Bruxelles, la police fédérale construit sa nouvelle unité OSINT'. *Intelligence Online*. 02/05/2023. URL: www.intelligenceonline.fr/surveillance--interception/2023/05/02/a-bruxelles-la-police-federale-construit-sa-nouvelle-unite-OSINT ,109949442-art
158 'Unit 8200'. *Wikipedia*. URL: wikipedia.org/wiki/Unit_8200
159 Geoff Brumfiel. 'Israel is using an AI system to find targets in Gaza. Experts say it's just the start.' *NPR.* 14 December 2023. URL: www.npr.org/2023/12/14/1218643254/israel-is-using-an-ai-system-to-find-targets-in-gaza-experts-say-its-just-the-st
160 Harry Davies, Bethan McKernan, Dan Sabbagh. 'The Gospel': how Israel uses AI to select bombing targets in Gaza.' *The Guardian. 1 December 2023.* URL: www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets
161 NicheRMS365 company. URL: nicherms.com/about-us
162 Interionet company. URL: www.interionet.com
163 Lars Bové and Jean-Paul Bombaerts. 'La police entame une révolution digitale à 300 millions d'euros.' *L'Echo*. 7 May 2022. URL: www.lecho.be/economie-politique/belgique/general/la-police-entame-une-revolution-digitale-a-300-millions-d-euros/10386480.html
164 Interview with a Senior Advisor r&d and ict Strategy Belgian Federal Judicial Police, 16/06/2023.
165 Becky Peterson. 'The founders of a billion-dollar Israeli spyware startup accused of helping Saudi Arabia attack dissidents are funding a web of new companies that hack into smart speakers, routers, and other devices'. *Business Insider*. 9 May 2019. URL: businessinsider.com/inside-the-israel-offensive-cybersecurity-world-funded-by-nso-group-2019-8

Despite this attempt to regain purity, Interionet is nonetheless the target of a boycott campaign. The Boycott, Divestment and Sanctions (BDS) movement works to end international support for Israel's oppression of Palestinians and to pressure Israel to comply with international law. It urges Belgians to oppose the contract between the Belgian Federal Police and Interionet, due to the company's use of Palestinians as test subjects for its surveillance software before marketing it globally.[166] Such a practice is not uncommon, as revealed in a recent book by journalist Antony Loewenstein: "Israel's military industrial complex uses the occupied, Palestinian territories as a testing ground for weaponry and surveillance technology that they then export around the world to despots and democracies".[167]

Figure 12. BDS movement Facebook post of 4 November 2022.
The description reads: Palestinians call for pressure to cancel Belgian police contract with Israeli spyware company Interionet. The company hides that it's based in apartheid Israel & that its facial recognition technology was tested on Palestinians. #MilitaryEmbargo #BanSpyware #IsraelOutOfMyPhone

Understanding exactly which companies are subcontractors for i-Police is challenging. Despite submitting freedom of information (FOI) requests, our efforts to obtain information about subcontractors and their software have been unsuccessful. Access to information was denied by invoking the need for commercial secrecy, or concerns that divulging excessive details about the platform's architecture might compromise its security.

Julie Chanson, a Federal Member of Parliament for the Green Party, fared no better when she asked about the project in April 2023:

> "Under the previous government, the public contract for the new i-Police platform was awarded to Sopra Steria. [...] However, suspicions have been raised about the seriousness of some [...] subcontractors. [...] These subcontractors may [have] close links to the former NSO Group [...]. I am

166 BDS Movement. 'Don't let the Belgian police use Israeli apartheid surveillance against Belgians!'. *Facebook*. URL: www.facebook.com/BDSNationalCommittee/photos/a.129952410382961/5947579748620169
167 Antony Loewenstein. 2023. *The Palestine laboratory: How Israel Exports the Technology of Occupation Around the World*. Verso Books. URL: www.versobooks.com/en-gb/products/2684-the-palestine-laboratory

> concerned about the reliability of such a strategic platform as i-Police and the data protection it must necessarily entail. Can you provide a full list of Sopra Steria's sub-contractors?"[168]

The answer from Minister of Interior Verlinden was evasive, and she refused to provide the contractors:

> "The list of subcontractors cannot be disclosed for the time being [...] taking into account the aspects of secrecy and confidentiality on the one hand, and the security aspects of the i-Police solution on the other hand. In the context of this public contract, the necessary checks on the right of access and the grounds for exclusion were carried out [...]. Consequently, there were no legal grounds to exclude the company or any of its partners from participating in this public contract".[169]

In a 2017 report on big data, the Belgian Data Protection Authority recommended that the COC be given a specific mission to evaluate the appropriateness and effectiveness of the i-Police project.[170] When we asked the head of the COC for their opinion on the involvement of controversial subcontractors within the i-Police project, they stated:

> "We do not monitor all contracts. [...] That is the responsibility of the Ministry of the Interior and of the Ministry of Justice, they are the ones who sign the contracts at the end of the day. Given the limited capacity we have, we are not able to control everything. We are able to carry out three to five proactive investigations a year, no more. [...]
>
> You are worried about Israeli companies, but there is not much choice, the Israelis are very efficient. When I talk to the people in charge of the Criminal Investigation Department, they say that if you want efficient software, there is not much alternative, in many cases only the Israelis are able to provide this type of software. [...]
>
> [Data protection] is always a problem, not just with the Israelis, already with Microsoft! [...] What guarantees are there that data won't be sent to the United States? The solution chosen is to impose a contractual obligation to keep the data in the European Union. But will the NSA respect these contracts? Nothing is less certain, as we have seen with Snowden's revelations".[171]

In June 2023, Minister of Interior Verlinden nonetheless tried to reassure the Parliament, arguing that the Federal Police collaborated with Europol to evaluate its methods based on AI and to apply the Accountability Principles for Artificial Intelligence (AP4AI).[172,173] The AP4AI principles claim to "constitute a universal, empirical-

168 Minister Verlinden's answer to the question 1775 by Julie Chanson, a green member of the Federal Parliament. 12/04/2023. URL: www.lachambre.be/kvvcr/showpage.cfm?section=qrva&language=fr&cfm=qrvaXml.cfm?legislat=55&dossierID=55-B108-1192-1775-2022202319320.xml

169 Minister Verlinden's answer to the question 1775 by Julie Chanson, a green member of the Federal Parliament. 12/04/2023. URL: www.lachambre.be/kvvcr/showpage.cfm?section=qrva&language=fr&cfm=qrvaXml.cfm?legislat=55&dossierID=55-B108-1192-1775-2022202319320.xml

170 CPVP. *Rapport Big Data*. 2017. p. 56. URL: www.autoriteprotectiondonnees.be/publications/rapport-big-data.pdf

171 Second interview with Frank Schuermans (COC), 11/10/2023.

172 Accountability Principles for Artificial Intelligence. URL: ap4ai.eu

173 Minister Verlinden's answer to question 1911 by Daniel Seneseal, a socialist member of the Federal Parliament. 26/06/2023. URL: www.lachambre.be/kvvcr/showpage.cfm?section=qrva&language=fr&cfm=qrvaXml.cfm?legislat=55&dossierID=55-B114-1192-1911-2022202320533.xml

ly validated Framework for AI in the law enforcement and justice sector to fundamentally assess and enforce legitimate and acceptable usage of AI by the internal security community".[174] The principles include:

- Universality: Every aspect of AI use can be monitored and assessed.
- Explainability: All AI practices, systems and decisions can be fully explained to the public and oversight bodies.
- Transparency: Information to assess AI use is easily and fully accessible.
- Independence: Groups that monitor and enforce are independent from Law Enforcement Agencies + AI developers.
- Compellability: It is possible to compel Law Enforcement Agencies to provide necessary information, systems or individuals to judge their AI use.
- Commitment to robust evidence: Law Enforcement Agencies are committed to providing robust evidence to judge their AI use.
- Pluralism: Every group involved in and affected by AI use has a voice.
- Enforceability and Redress: It is possible to compel Law Enforcement Agencies to comply with all requests to improve their AI practices.

One does not know whether to laugh or cry at the gap between these principles and the current level of accountability displayed by Belgian authorities – especially considering that all of these programmes rely on algorithms with closed code protected by intellectual property, making it impossible to ascertain precisely how they function.

Furthermore, even if the code were accessible and it were possible to discuss the methods with the software developers, it might not be possible to understand how they work. More and more algorithms are built with complex machine learning methods. Machine learning models are often referred to as 'black boxes'. This means that a model operates as an opaque system where the internal workings are unclear, both to researchers and users.[175] The 'black box problem' can lead to software perpetuating biases and prejudiced power structures, with no clear identification of the origin of and solution to the issue.

What's more, closed-code systems may contain 'backdoors', enabling software manufacturers to access them remotely. This practice is prevalent among Israeli suppliers. The Federal Police recently learned this the hard way. According to police union representatives with whom we spoke, the Federal Police had to make an urgent replacement of their phone-tapping provider, after discovering they were not the only ones listening in on their suspects. In case you were wondering "who watches the watchers?", now you know.

174 The AP4AI Principles. URL: ap4ai.eu/about/principles
175 Lou Blouin, 'AI's mysterious 'black box' problem, explained'. University of Michigan-Dearborn. 6 March 2023. URL: umdearborn.edu/news/ais-mysterious-black-box-problem-explained

4. The i-Police programme: state of progress

In August 2023, the Minister of Interior reported to the Federal Parliament on the progress made by the i-Police project[176] The project started by implementing a process to exchange data internationally: at the time of the Minister's statement, the integration of the EU's Schengen Information System (SIS) was being finalised, with Europol and Interpol to follow in 2024.

A second project was also part of the initial i-Police roll-out. This involved processing data from the ISLP and the BNG-ANG databases for information-led policing (ILP) which lies at the core of the i-Police initiative. According to the tender:

> "The purpose of ILP consists in gathering or consulting data (raw data), to convert them into new insights and, based on those insights, to better steer and manage the operation of the three other domains. Raw data processed by ILP can originate from different channels and sources:
>
> - data generated by the operational functioning of the police;
> - data provided by partners of the police or transferred by third parties to the police (external data sources);
> - data that are publicly accessible and are picked up by the police.
>
> These data are then converted by ILP into 'Intelligence' or 'insights'. These insights should be in timely, accurate, valuable, action-oriented, and are designed to guide and steer the operations. Depending on the type of direction, we speak of operational intelligence, tactical intelligence and strategic intelligence".[177]

A pilot phase of the ILP project was launched at the end of 2023. It took place in the province of Liège and involved both the local and Federal Police. The aim of the pilot phase was said to identify areas for attention and improvement before moving forward in 2024.[178]

However, recent reports in Belgium note that the development and implementation of the system was beset with problems. One report in *De Tijd* claims that the UK consultancy company Deloitte carried out a stringent audit. According to the paper, this concluded that the digital transformation of the police is not streamlined, resulting in a fragmented approach, and that there is inadequate internal control over the way police staff use and maintain the database. This may lead to misuse.[179] The authors of the audit spoke in the Federal Parliament and declared:

> "In terms of standards and legislation, we found that there was not really any formalised management of information about the operational use of data, security and privacy. We also found that there was no real strategy for information security and no action plan for implementation. [...]

176 Minister Verlinden's answer to question 1964 by Daniel Seneseal, a socialist member of the Federal Parliament. 31/08/2023. URL: www.lachambre.be/kvvcr/showpage.cfm?section=qrva&language=fr&cfm=qrvaXml.cfm?legislat=55&dossierID=55-B117-1192-1964-2022202320932.xml

177 GPI. 2020. *i-Police tender. Appendix H – Context and scope of the tender*. p. 24.

178 Minister Verlinden's answer to question 1964 by Daniel Seneseal, a socialist member of the Federal Parliament. 31/08/2023. URL: www.lachambre.be/kvvcr/showpage.cfm?section=qrva&language=fr&cfm=qrvaXml.cfm?legislat=55&dossierID=55-B117-1192-1964-2022202320932.xml

179 Stéphanie Romans. 'Audit kraakt digitale transformatie van politie'. *De Tijd*. 31/05/2023. URL: tijd.be/politiek-economie/belgie/federaal/audit-kraakt-digitale-transformatie-van-politie/10471186.html

> We have found that internal management control is limited and inadequate when it comes to information management. So it is important to put management control processes in place because we are talking about strictly private data".[180]

Another report in *Le Soir* warned that the Federal Police can no longer pay their bills and that the total amount outstanding is several tens of millions of euros. The paper adds: "Some consultants – particularly in the IT sector – are no longer being paid and are beginning to insist on being duly honoured".[181] According to a union representative with whom we spoke, the i-Police project is presently undergoing serious revisions to prioritise the stability of fundamental IT police operations, significantly reducing the project's initial aspirations.

All of this raises questions about the role of private companies offering consultancy services to the apparently-bankrupt Federal Police. The Federal Police commissioned Sopra Steria/KPMG to develop i-Police, only to later commission Deloitte to audit the process, leading to the conclusion that there is a deficiency in internal strategy. It remains to be seen whether other private companies will benefit further from this process. No doubt there are many who would be willing help draft a new strategy.

It is unclear which recounting of events can be trusted. Should we believe the police's claim that they are using high-tech systems that process all the data and miraculously point to criminals? Or should we side with Deloitte's conclusion that the police are poorly organised and depend on outdated software?

In an interview, the Chair of the COC, Frank Schuermans, said the following about i-Police:

> "The police are not nearly as efficient as people think. [...] i-Police is all talk, at least for now. The situation with the CCTV cameras leaves no room for any other interpretation. We are announcing that we are going to put ANPR cameras everywhere, that there will be 10,000 new cameras, but we cannot connect the 1,500 ANPR cameras that are already there or set up a logging system on those cameras. It's all just window dressing! There is a huge gap between communication and the situation in the field. The typical example is the AMS (ANPR Managed Services)[182], where we cannot keep track of the number of cameras that need to be connected because of huge technical problems. It's a load of rubbish".[183]

It is reassuring to know that the police's level of technological sophistication may not match their proclaimed capabilities. Nevertheless, the development of i-Police will have to be closely monitored, as things can move very fast when it comes to police uses of technology. It will also be important to ensure that, if the i-Police project is discontinued, some of its most intrusive components are not simply rebranded and put back into use.

180 Hearing at the Federal Parliament of Deloitte inspectors following their audit of the IT department of the Federal Police. Chambre des représentants de Belgique. Doc 55 3516/001. URL: www.lachambre.be/media/index.html?language=fr&sid=55U4143#video

181 Xavier Counasse. 'La police fédérale ne peut plus payer ses factures'. *Le Soir*. 16/08/2023. URL: lesoir.be/531380/article/2023-08-16/la-police-federale-ne-peut-plus-payer-ses-factures

182 Sometimes also referred to as ANPR Management Software.

183 Second interview with Frank Schuermans (COC), 11/10/2023.

Automating justice in Belgium: small steps, major issues

In legal settings around the world, algorithms are increasingly used to anticipate decisions in future cases and predict judicial outcomes by processing vast amounts of data (legislation, case law, and doctrine).[184] 'Predictive' justice is expected to have numerous functions, including providing individuals with insight into their odds of success in legal proceedings, and aiding judges in decision-making.

The implementation of automated decision-making systems and AI in the legal sector in Belgium is significantly hindered by a lack of access to the data needed to train such tools. The persistent dependence on analogue communication practices within the Belgian legal system renders the prompt implementation of AI improbable.

However, civil law courts have conducted experiments in ai-powered legal advice,[185] university researchers are exploring the development of AI methods adapted to Belgian law,[186] and recent legislation mandates the creation of a central register for court decisions, which would allow for the training of AI software.[187] All of this raises concerns about the automation of aspects of the justice process, and extension to criminal courts, and eventually the possibility of algorithm-driven court decisions that could remove individuals from the courtroom, potentially compromising transparency and contestability.[188]

A report published in December 2024 by the Belgian Court of Audit provides a comprehensive analysis of the digital strategy within Belgium's justice system.[189] It identifies substantial shortcomings in the approach to digital transformation. A key criticism is that despite the Ministry of Justice earmarking no less than €140 million specifically for digitisation in 2023, it was unable to develop a unified and coherent strategy. The report also highlights risks associated with consultancy projects, including budget management, conflicts of interest, and commercial influence.

The development of 'predictive' justice in the legal system is not progressing as fast as that of the police. However, it appears to exhibit a number of the same pitfalls.

184 Matthias Van Der Haegen. 2023. 'Quantitative Legal Prediction: The Future of Dispute Resolution?' in De Bruyne & Vanleenhove (eds.). *Artificial Inteligence and the Law*. Second Revised Edition. Chapter 4. pp. 83-110.

185 Alain de Fooz. 'Legal Insights: Les avocats peuvent accéder à l'intelligence artificielle !' *Solutions Magazine*. 07/03/2018. URL: solutions-magazine.com/legal-insights-avocats-intelligence-artificielle

186 Gregory Lewkowicz. 'Cross-jurisdictional AI Methods for Civil Law Court Decisions'. *LinkedIn*. June 2023. URL: linkedin.com/posts/gregory-lewkowicz_intelligenceartificielle-droitcivil-activity-7066291630386880512-GQHn

187 Loi du 16 octobre 2022 visant la création du Registre central pour les décisions de l'ordre judiciaire et relative à la publication des jugements et modifiant la procédure d'assises relative à la récusation des jurés. URL: www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=22-10-24&numac=2022033790

188 Rémy Farge & Emmanuelle Hardy. 2023. 'Justice : prédire la place de l'IA'. *La chronique des droits humains*. No. 203. URL: www.liguedh.be/wp-content/uploads/2023/07/2-Justice.pdf

189 Cour des comptes. 2024. *Pilotage de la transformation numérique de la justice par l'État fédéral*. URL: www.ccrek.be/fr/publication/pilotage-de-la-transformation-numerique-de-la-justice-par

Conclusion: *Garbage in, garbage out*

The main insights of this report are briefly outlined below. The findings are then discussed with policy recommendations for appropriate governance of AI and automated decision-making in policing and criminal legal settings. This includes a recommendation for an outright prohibition on 'predictive' policing, as well as obligations around transparency, accountability, fairness.

1. Summary

I. The local police forces in Belgium possess significant autonomy, resulting in various 'predictive' policing initiatives in different areas.

A lack of transparency makes it impossible to get a complete picture of the actual functioning of these systems. Nonetheless, it is clear that many police forces use basic 'hotspot' geographic systems. A few police forces have proudly claimed to implement 'predictive' policing methods: Westkust, Zennevallei, and Antwerp. Most notably, Antwerp police, who are at the forefront of automation among local police forces, have developed their in-house FOCUS mobile application. This is supposed to give officers in the street instant access to a wide range of data sources. It has since been distributed to other forces across the country, before being selected as the fundamental interface for the federal i-Police project.

II. 'Predictive' policing systems will rely on police databases.

However, Belgian police databases – which are numerous – are poorly maintained, and often do not comply with the law. Police databases already severely impact individuals. Errors and unjust classifications have the potential to result in unwarranted searches, heightened airport security checks, and compromised professional activities. Misinformation often results in damaging a person's reputation and livelihood.

Moreover, the policing of sex work and so-called urban 'gangs', alongside anti-radicalisation policies, disproportionately target marginalised groups and reinforce existing structural inequalities. Without serious countermeasures, the automation of policing is bound to exacerbate these issues. The absence of rights for people to directly access their data and meaningful avenues for appeal, as well as the lack of any other protective framework, mean that people and groups impacted cannot challenge them or seek redress.

III. i-Police is a plan launched by the Federal Police for a major overhaul of its outdated IT infrastructure.

This € 300 million project aims to automatically analyse and cross-reference a range of data types: local, federal and international police databases, as well as CCTV footage and external sources. Data and analyses of it are then supposed to be made widely available to officers in the street and in police stations.

1. The i-Police programme raises several legitimate concerns, particularly regarding the centralisation of large amounts of data on a single **data lake** and the use of opaque algorithms.

   The 'data lake' raises concerns for potential loss of distinction between 'validated' and 'non-validated' information. In computer science, the 'garbage in, garbage out' principle indicates that flawed input data cannot produce reliable output. This is a major concern with i-Police's data lake.

2. i-Police is set to integrate **video surveillance** footage.

   This raises several concerns, as the Belgian police have repeatedly broken the law on video surveillance. Whether it is facial recognition technology usage at Brussels airport or employing Clearview AI software for detecting criminals, the Belgian police appear fixated on the possibilities presented by new technological advancements rather than complying with the minimum legal requirements. Given the government's plan to legalise face recognition and to implement ANPR cameras across the country, there is reason to worry (and take action).

3. The i-Police programme plans to utilise and analyse external sources, a practice known as **open-source intelligence** (OSINT). There is a lack of clarity regarding which companies will participate in the project and the software employed. The main contractor for i-Police is Sopra Steria, with support from consultancy company KPMG. The analysis of the data will depend on confidential algorithms provided by private and overseas contractors, whose ethical practices are questionable.

4. Despite significant advances in recent years, Belgium has encountered obstacles with the 'i-Police' initiative.

   An external audit found the digital transformation of the police disjointed, with a lack of internal control, security, and privacy measures. This is particularly worrisome given the large amounts of confidential information involved. Moreover, the Federal Police faces financial difficulties, with debts totalling tens of millions of euros. Hence, the i-Police project is likely to be subjected to revisions, with a focus on ensuring the stability of core IT police operations.

2. Discussion

Digitisation and automation in the police and justice domains in Belgium follow different paths for law enforcement and legal proceedings. There is a greater adoption of technology in policing than in legal settings. Both settings however, raise concerns about potential infringements on fundamental rights, and reinforced discrimination and criminalisation. As such, ongoing vigilance and anticipation of digitisation is paramount.

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.[190]

A lack of transparency and accountability, and no access to effective remedies,

190 *Ibid.*

compounds these issues. 'Predictive' AI systems 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.[191]

Furthermore, 'predictive' systems infringe upon core principles of justice, including the presumption of innocence; the right to privacy, to liberty and to a fair trial; the freedom of assembly and association; and equal treatment before the law. Individuals, groups, and locations are prematurely labelled as potential threats, leading 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.[192]

Meanwhile, human rights assessments or basic cost-benefit analyses are nowhere to be found in the testing of Belgian 'predictive' systems. The absence of any pre-deployment evaluation based on the system's potential to cause harm raises doubts about the efficiency, proportionality, necessity, and long-term consequences of these measures. It would be imperative to understand the impacts of 'predictive' policing before blindly embracing it.

When asked whether 'predictive' policing should be allowed in Belgium, Frank Schuermans, from the COC, answered:

> "That's a very difficult question. That's first and foremost a question for the legislator and for the parliament [...]. I am at this stage very reluctant to say yes, to that question. Not so much, because of the principle that it should not be possible, but of the daily experience that we have; from our day to day work we see that there is a huge issue of accuracy of police data. Even now, without big data. And precisely because that would be the basis of all systems of profiling".[193]

At present, there are urgent and ongoing discussions among civil society, policymakers, and academics about the regulation of ai, including in policing, to minimise the potential for harm. In Belgium, an academic researcher at KU Leuven, Thomas Marquenie, has proposed a set of guidelines for regulating AI. He emphasises:

- the imperative of complying with data protection law, particularly through the systematic recourse to data protection impact assessments (DPIA);
- the need for profiling restrictions and limitations on the use of sensitive data;
- the importance of always having a 'human in the loop' to uphold the principles of accountability and liability;
- the need for a higher level of public transparency: authorities should inform citizens and share information on the tools they use and the data they process;
- that the use of AI should be limited to defined purposes, profiles, and situations.[194]

191 Debailleul, Corentin, Jérémy Grosman and Aline Wavreille. 2022. « Repolitiser l'usage des algorithmes ». in *État des droits humains en Belgique – Rapport 2021*. Brussels: Ligue des droits humains.URL: www.liguedh.be/wp-content/uploads/2022/01/Classeur7.pdf

192 Fair Trials. 2021. *Automating Injustice: The Use of Artificial Intelligence and Automated Decision-Making in Criminal Justice in Europe*. URL: www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf

193 Interview with Frank Schuermans (COC), 17/02/2023.

194 Thomas Marquenie. 2022. 'Het gebruik van AI-toepassingen binnen het politiewezen: voordelen, risi-

Obviously, the use of AI must also always have a legal basis, and the police should engage in consultation with the Supervisory Body (COC) prior to implementing new systems or tools. Marquenie's proposals seem only reasonable. Additions to his proposals could be validated police files, rigorous data minimisation practices and regular audits as minimum requirements for the development of any 'data-driven solution'.

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 alone.

It is a fallacy to believe that the Belgian police will duly respect legal frameworks for regulating AI. There are numerous examples of law enforcement authorities failing to uphold existing requirements on police use of data and algorithms. For example, COC reports on facial recognition at the Brussels airport, on Clearview AI, and on the BNG-ANG database prove that the Federal Police disregard the law on a daily basis. This points to structural problems that cannot be solved immediately.

Moreover, there are serious concerns about the accuracy of police data. This context jeopardises any hope of fair usage of 'predictive' policing tools in Belgium. In such an environment, one can only question the validity of investing in 'predictive' policing tools.

Additionally, 'predictive' policing relies on the assumption that certain locations or individuals are inherently prone to criminal activities. These assumptions are based on criminological theories that lack empirical support and oversimplify the complex nature of crime causation.

Hence it appears only reasonable to frankly oppose the development of 'predictive' policing tools in Belgium. As a recent thesis on i-Police concludes:

> "Existing solutions to limit the damage have been mentioned above. But let's not kid ourselves: these solutions ultimately act as lifebuoys when it is the ship that needs to be prevented from sinking. The use of predictive policing is nonsense [...]. Worse than nonsense, it is in many ways a danger that should not be underestimated because of the falsely neutral appearance given to the technologies. The time, energy and money invested in these tools could have been better spent on education [...] or tackling inequality, which are sustainable ways of tackling crime. Some people will call me a utopian, but where is the utopia in claiming to be able to predict crime?"[195]

co's en best practices'. Staten Generaal over Artificiële Intelligentie. *Centre for IT & IP Law (CiTiP)*. 17 June 2022. URL: vaia.be/files/cursusmateriaal/presentaties/220617-3-Thomas-Marquenie.pdf

195 Jérémiah Vervoort, 2021. *I-Police ou l'art de prédire la discrimination*. Master's Thesis. Bruxelles: Université libre de Bruxelles.

A prohibition on 'predictive' policing directly opposes the approach pursued by the Permanent Committee of the Local Police (CPPL-VCLP), the umbrella organisation of the local police forces. In its vision document *Horizon 2025,* the Committee states:

> "Despite all the transformations in support of intelligence-led policing (i-Police, FOCUS, ANPR, etc.), we are still only on the eve of this revolution. The future possibilities are endless, culminating in the evolution towards predictive policing based on big data and data mining. Every day, we come up against the limits of the concepts of 'privacy' and 'human rights'. The debate on privacy must be conducted as a matter of urgency, with the following basic principle: 'Harnessing information and technology to improve the quality of life and security of citizens!'"[196]

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.

In conclusion, 'predictive' policing, as it stands in Belgium, is far from being a responsible, effective, or ethical endeavour. It is paramount that we challenge its adoption, with a resolute commitment to protect our rights and freedom. It is essential that we raise our voices in opposition to 'predictive' policing. Prohibiting 'predictive' policing and automated decision-making in criminal justice is a step towards a future where justice and equality are not compromised in the name of technological innovation. It is an assertion that the rights and well-being of its people are paramount, and that we stand firmly against any technology that undermines these principles.

196 CPPL-VCLP, 2019. Horizon 2025. Commission Permanente de la Police Locale. p. 13. URL: www.police.be/5806/sites/5806/files/downloads/HORIZON%202025%20FR_0.pdf

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
CC-BY-SA Corentin Debailleul, 2023