



# PETIT PAYS, BIG DATA

Automatisation de la discrimination et police "prédictive" en Belgique

**AVRIL 2025** 

## **-**STATEWATCH





European
Artificial Intelligence
& Society Fund



tac tiC

### Méthodologie

Auteur principal: Corentin Debailleul.

**Supervision, relecture et édition** par Griff Ferris et Sofia Lyall.

**Recherches documentaires** effectuées par Nathalie Vandevelde, Maria Karantoumani, Griff Ferris, Sofia Lyall et Corentin Debailleul.

Un **questionnaire** sur l'utilisation de bases de données spécifiques a été envoyée à une série de zones de police locales identifiées comme des cibles stratégiques. L'enquête a été préparée collectivement et réalisée par Nathalie Vandevelde.

Des **demandes d'accès** ont été envoyées par la commission "Nouvelles technologies et vie privée" de la *Ligue des droits humains* (LDH) à toutes les zones de police locale et autorités communales francophones, ainsi qu'aux plus grandes villes flamandes (Gand et Anvers), concernant les dispositifs de surveillance et leurs emplacements, les documents relatifs aux marchés publics et les analyses d'impact relative à la protection des données (AIPD) correspondantes. Des demandes d'accès ont également été envoyées à la Police Fédérale, concernant i-Police et la reconnaissance faciale.

Les informations ont été vérifiées par **triangulation** sur base de la presse, des sites web dédiés aux marchés publics, des procès-verbaux des débats parlementaires et des conseils communaux et de police.

**Entretiens** réalisés par Griff Ferris et Sofia Lyall :

Date	Nom et/ou poste
2023-02-17	Frank Schuermans, directeur de l'Organe de contrôle de l'information policière (COC)
2023-04-04	Catherine Forget, avocate et chercheuse en droit, spécialisée notamment dans les bases de données policières

#### Entretiens réalisés par Corentin Debailleul :

Date	Nom et/ou poste
2023-06-16	Commissaire principal de la police judiciaire fédérale, conseiller principal en R&D et en stratégie TIC auprès du directeur général de la police judiciaire fédérale
2023-06-28	Gregory Lewkowicz, Professeur de droit à l'université (ULB) participant à un programme de recherche visant à mettre au point un logiciel d'intelligence artificielle (IA).
2023-07-03	DPD d'une zone de police locale
2023-08-04	Coordinateur d'une association soutenant les travailleurs·euses du sexe masculins et trans (Bruxelles)

2023-08-08	Nina Henkens & Onur Cevik, Travailleur∙euse sociaux chez Kif Kif (Anvers)
2023-08-17	Délégués syndicaux, Police Fédérale
2023-09-19	Un juriste, ancien collaborateur de la Police Fédérale
2023-09-28	Farah Kassem, chercheuse à la KU Leuven sur la (dé)radicalisation
2023-10-11	Frank Schuermans, directeur de l'Organe de contrôle de l'information policière (COC)

Enfin, des discussions informelles ont eu lieu avec des membres de la commission Nouvelles technologies et Vie privée de la Ligue des droits humains; des membres du collectif Technopolice Bruxelles; un travailleur social d'Anvers travaillant avec des personnes trans travailleuses du sexe; une conseillère politique chez UTSOPI; une source au sein de la Police Fédérale; et finalement une avocate, membre de l'Observatoire international des prisons – section belge.

**Traduction depuis l'anglais** par Emmanuelle de Buisseret Hardy et Corentin Debailleul, aidés par DeepL.

**Relecture** par Emmanuelle de Buisseret Hardy, Manuel Lambert, Rémy Farge, Fien De Meyer, Chris Jones et Sarah De Laet.

Contact: corentin.debailleul@ulb.be

Mise en page par Margaux Hallot.



### Résumé

En Belgique, comme ailleurs dans le monde, la police s'appuie de plus en plus sur l'exploitation des données pour tenter de "prédire" les crimes et délits. Le bénéfice attendu serait l'amélioration de "l'efficience" et de "l'efficacité" de la police par la maîtrise des algorithmes, des données et de "l'innovation".

Cependant, cette nouvelle ère numérique peine à advenir et fait face à quelques obstacles. Les données policières sont souvent inexactes et reflètent les biais systémiques présents dans la police comme dans la société – en particulier le racisme, l'islamophobie et le classisme.

Les lois, les procédures et les systèmes en place ne permettent pas réellement de contrôler comment les données sont collectées, stockées, partagées et utilisées. Les personnes concernées n'ont que peu de voies de recours, ou si défaillantes qu'elles en deviennent inutiles.

Le présent rapport aborde ces graves problèmes en analysant trois grands thèmes :

- les systèmes de police "prédictive" utilisés par les zones de police locales;
- les bases de données utilisées pour alimenter ces systèmes ;
- le projet "i-Police" de la Police Fédérale, conçu pour utiliser les données de la police et d'autres organismes publics, ainsi qu'une série d'autres sources de données, afin d'éclairer les décisions et les activités de la police.

#### Police "prédictive"

Les techniques de profilage et de police "prédictive" s'appuient sur les algorithmes et l'analyse des données pour soi-disant "prédire" puis chercher à "prévenir" de potentielles activités criminelles.

Les objectifs affichés sont les suivants :

- allouer les ressources policières de manière plus efficace en anticipant et en devançant l'activité criminelle dans certains lieux ou zones;
- identifier des "zones à risque" et profiler des individus en tant que criminels (potentiels) afin de les surveiller de plus près ;
- justifier des interventions policières telles qu'une interpellation, une fouille, un interrogatoire, ou une arrestation.

#### Zones de police locales

Différents outils et systèmes sont utilisés par les zones de police locales belges à ces fins. Le système d'information géographique Orbit, produit par la société gantoise Columba, est particulièrement répandu. Il utilise les données géographiques de criminalité pour identifier de prétendus "points chauds" (*hotspots*). L'entreprise affirme que son logiciel est utilisé par près de cent zones de police en Belgique.

La zone de police Westkust couvre les communes flamandes de La Panne, Coxyde et Nieuport, et a été précurseure du processus de numérisation de la police. Une visite du chef de la police locale aux États-Unis a inspiré un plan visant à utiliser les données policières pour « prévoir grosso modo où les choses pourraient mal tourner », selon les termes du commissaire.¹ Le système aurait entraîné une réduction de 40 % des incidents criminels, mais il n'y a pas eu d'évaluation objective du système ou de son fonctionnement.

La zone de police Zennevallei couvre les municipalités de Beersel, Hal et Leeuw-Saint-Pierre dans la banlieue flamande au sud-ouest de Bruxelles. Son intérêt pour la police "prédictive" a conduit à un projet avec l'Université de Gand, conçu pour "prédire" les cambriolages. Le modèle était basé sur l'exploitation des données de criminalité mais aussi d'autres variables, telles que les conditions météorologiques.

Leur méthode est basée sur la modélisation de "zones à risque" (*Risk Terrain Modelling* – RTM), pour tenter d'identifier les quartiers potentiellement plus exposés aux activités criminelles, en raison de "facteurs environnementaux". Cependant, les théories criminologiques qui sous-tendent cette approche ont été largement critiquées dans la mesure où elles négligent les facteurs complexes, multiples et structurels de la criminalité. Pour améliorer le fonctionnement du système, les chercheurs à l'origine du projet appellent de leurs vœux l'exploitation de toujours plus de données, notamment issues des réseaux sociaux, et bénéficient pour cela de fonds européens.

Dans la ville portuaire d'Anvers, la police a acquis des caméras-piétons (*bodycams*) dans le cadre d'un marché conclu avec l'entreprise suédoise Securitas. Cette entreprise a également repris certaines activités de la police d'Anvers, telles que le contrôle des images de vidéosurveillance.

Par ailleurs, la police anversoise a développé sa propre application pour smartphone, appelée FOCUS. Cette application permet aux agents de terrain d'accéder aux fichiers de police et de bénéficier de nombreuses autres fonctionnalités, comme une carte interactive, une messagerie ou un bloc-note. Parallèlement, la zone de police centralise sur une plateforme unique des données provenant de sources multiples : systèmes ANPR, localisation des voitures de police, images de vidéosurveillance, et signaux issus des téléphones portables pour la gestion de foules. Des techniques d'analyse avancée y sont également appliquées aux images

<sup>1</sup> 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/

de vidéosurveillance, notamment la reconnaissance de texte, le profilage comportemental et le suivi d'objets.

Ces systèmes, outils et techniques ont été discréditées au vu des questions qu'elles soulèvent relativement à la protection des libertés publiques et des droits humains. Il a été démontré dans plusieurs contextes que la surveillance policière ciblée sur des "points chauds" perpétue des schémas discriminatoires et une surveillance policière exacerbée de certaines personnes ou quartiers. L'intégration d'un nombre croissant de sources de données aggrave ces problèmes, et en amène d'autres concernant la vie privée, le principe de minimisation des données et le risque d'utilisation abusive ou de fuites.

Les systèmes "prédictifs" tels que ceux utilisés par les zones de police locales en Belgique portent atteinte aux principes fondamentaux de justice, notamment le droit à la liberté, le droit à un procès équitable et la présomption d'innocence. Pour des motifs discutables, des individus, des groupes et des lieux sont étiquetés comme des menaces potentielles. Cela peut conduire à des mesures préventives punitives, telles que des privations de liberté injustifiées. Cela érode le principe essentiel selon lequel les individus sont considérés comme innocents jusqu'à ce que leur culpabilité soit prouvée, et pose un grave risque d'erreurs judiciaires.

#### Bases de données policières

La plupart des données utiles aux systèmes de police "prédictive" proviennent des bases de données policières. En Belgique, celles-ci posent un problème fondamental dans la mesure où leur création, leur contenu et leur usage ne font pas l'objet d'un contrôle efficace. Les lois sur la protection des données ne sont que partiellement appliquées. Les agent·es qui accèdent illégalement à des données ne font peu ou pas l'objet de sanctions.

Ce manque de contrôle et de supervision est d'autant plus frappant en Belgique que les bases de données policières y sont innombrables et que l'éventail des données qu'elles peuvent contenir est extrêmement large. De plus, ces données sont souvent imprécises ou inexactes mais surtout récoltées et structurées par les biais systémiques de la police et de la société dans laquelle elle intervient.

Les informations contenues dans les fichiers peuvent parfois n'être que ouï-dire, spéculations ou de pures inventions – comme dans le cas d'un homme dont la fiche affirmait qu'il prévoyait d'infecter des policiers avec le VIH. D'autre part, les bases de données peuvent également marginaliser davantage des personnes se trouvant dans des situations déjà difficiles, comme l'illustre l'exemple d'une application partagée par la Ville et la police d'Anvers et permettant d'enregistrer les travailleurs ses du sexe. Censée garantir leur sécurité, cette application risque d'éloigner des services et organisations de soutien les travailleurs ses du sexe au statut migratoire précaire, car l'enregistrement dans l'application pourrait finalement conduire à leur expulsion du territoire.

Les fichiers de police sont également consultés pour un nombre croissant de raisons différentes. Peu de gens s'étonneraient de leur consultation dans le cadre du recrutement des personnes susceptibles d'avoir accès à des informations classifiées ou à des zones sensibles telles que les sites nucléaires. En revanche, l'utilisation de ces bases de données pour contrôler les candidat·es bénévoles pour un festival de musique est plus inattendue.

Ce rapport relate l'expérience d'un jeune homme qui s'est vu refuser un emploi après avoir été arrêté et accusé à tort d'avoir participé à une manifestation. Cette accusation et cette arrestation lui valent encore d'être contrôlé et interrogé dans les aéroports. Des rapports indépendants font également état d'un nombre disproportionné d'habilitations de sécurité refusées aux travailleurs ses d'origine nord-africaine.

Les effets de ces politiques sont sérieux et variés. Des personnes ont subi des pertes financières et des difficultés à trouver un emploi. Ces difficultés financières exacerbent leur vulnérabilité aux préjudices et à la marginalisation. En outre, la législation belge n'offre pas de possibilité aux personnes d'accéder à leurs données, ce qui rend extrêmement difficile – voire impossible – la rectification ou la suppression des erreurs.

#### Le projet i-Police

En préparation depuis plus de dix ans, le projet i-Police est actuellement entre les mains de la Police Fédérale et de l'entreprise Sopra Steria, avec le soutien de la société de conseil KPMG et d'une série de sous-traitants. Parmi ces sous-traitants figurent un certain nombre d'entreprises israéliennes, y compris des entreprises dont les fondateurs ou dirigeants sont d'anciens responsables des services de renseignement militaire. Cela soulève de sérieuses questions sur les engagements éthiques des autorités belges, mais aussi sur la possibilité d'éventuelles "portes dérobées" (backdoors) qui permettraient un accès illégal à des données particulièrement sensibles.

D'après un communiqué du ministère de l'Intérieur :

i-Police propose une analyse et un recoupement automatiques des données, telles que les images des caméras, les photos, les empreintes digitales, les traces, les documents... Ces fonctionnalités permettent d'identifier plus rapidement et plus clairement les criminels et les phénomènes de criminalité. Les enquêteurs reçoivent une multitude d'informations filtrée en temps réel et peuvent ainsi agir rapidement et de manière ciblée. [...] En outre, le système offre aux citoyens une garantie de confidentialité et un contrôle transparent. Les fonctionnaires de police auront un accès limité et contrôlé aux informations des citoyens, sur la base de leur fonction et de leur mission à ce moment.<sup>2</sup>

<sup>2</sup> Annelies Verlinden. *i-Police: l'avenir de la police est numérique*. 7/05/2022. URL: verlinden.belgium.be/ fr/i-Police

Le projet prévoit un certain nombre de fonctions "prédictives" axées sur la localisation, ou encore la possibilité pour les agent·es de recevoir des notifications sur des suspects en temps réel – par exemple si ceux-ci sont repérés par une patrouille.

Aussi extravagants qu'ils puissent paraître, ce programme fédéral comme les systèmes développés par les zones de police locales reposent sur l'intégration et l'analyse de grandes quantités de données. Ces données devraient provenir d'agences gouvernementales nationales et internationales, d'entreprises privées et de sources accessibles au public telles que les réseaux sociaux ou la presse. Ces sources contiennent à la fois des informations vérifiées et non vérifiées. Outre les questions de proportionnalité et de nécessité, le problème se pose d'orienter l'action de la police sur des algorithmes biaisés, traitant des données en partie fondées sur des rumeurs. L'automatisation de l'analyse des séquences de vidéosurveillance, à la recherche d'activités "suspectes" soulève des problèmes similaires, ainsi que des questions sur l'intérêt fondamental de ces technologies pour une société prétendument démocratique.

Cependant, comme pour de nombreux projets publics de numérisation, le futur n'est pas si bien tracé que les premières annonces du projet i-Police ne le prétendaient. Des campagnes sont en cours contre l'utilisation de technologies israéliennes par la police belge ; les organes de contrôle sont très préoccupés par la collecte et l'utilisation inappropriées de données ; et la Police Fédérale belge est désargentée. Chacun de ces facteurs devrait suffire à remettre en question la nécessité d'un tel projet. Les trois combinés devraient, on l'espère, y mettre un terme une fois pour toutes. L'avenir nous le dira.

#### Pour une interdiction immédiate

Tout d'abord, les systèmes "prédictifs" sont connus pour cibler et discriminer de manière disproportionnée les groupes marginalisés, renforçant ainsi les inégalités structurelles existantes. Les données sur la prétendue race, la religion, le statut socioéconomique, le statut migratoire et la nationalité deviennent souvent des facteurs déterminants la surveillance et la criminalisation de certains groupes, voire l'acharnement contre ceux-ci. Elles sapent et violent de multiples principes fondamentaux comme la liberté de circulation et la présomption d'innocence, ou le droit à un procès équitable, et à l'absence de discrimination.

Le manque de transparence et de responsabilité, ainsi que l'absence de voies de recours efficaces, aggravent ces problèmes. Les systèmes "prédictifs" fonctionnent à l'abri de barrières technologiques et commerciales, soustrayant leurs décisions à tout examen public. Les personnes concernées sont laissées dans l'ignorance, sans moyen clair et efficace d'ouvrir les "boîtes noires" et de contester ces décisions opaques.

Le droit belge offre peu de protections significatives contre ces problèmes profondément enracinés, et encore moins de moyens de les résoudre. Le règlement européen sur l'intelligence artificielle (AI ACT) ne devrait pas être d'un grand secours à cet égard – d'autant plus dans un contexte où les autorités belges n'ont pas correctement appliqué la législation européenne existante censée protéger les individus, notamment sur la protection des données.

Les protections juridiques existantes doivent être appliquées et de nouveaux mécanismes juridiques doivent être introduits pour les compléter. Toutefois, ces propositions réglementaires ne sauraient être suffisantes pour éviter les préjudices que causerait la généralisation de la police "prédictive" Belgique. Ce rapport met en lumière des problèmes structurels de racisme, d'islamophobie et de classisme dans la police. Ces problèmes sont systémiques et ne peuvent être résolus par le seul encadrement de la gestion des données et des algorithmes de la police.

Au regard de tous ces enjeux, il est impératif que la Belgique interdise l'utilisation de systèmes de police "prédictive" et de prise de décision automatisée dans le cadre du maintien de l'ordre et de la justice pénale. En interdisant ces systèmes, la Belgique peut faire un pas important vers la construction d'une société plus équitable et plus juste. C'est l'occasion de réaffirmer son engagement à défendre les droits fondamentaux, à promouvoir l'égalité et à maintenir les principes de responsabilité et de justice.

## Acronymes et abréviations

AIPD	Analyse d'impact relative à la protection des données
ANPR	Automatic number plate recognition (Lecture automatique de plaques d'immatriculation – LAPI)
APD	Autorité de protection des données
BNG	Banque de données nationale générale
CERD	Comité des Nations unies pour l'élimination de la discrimination raciale
CJUE	Cour de justice de l'Union européenne
COC	Controleorgaan op de politionele informatie – Organe de contrôle de l'information policière
CPPL	Commission Permanente de la Police Locale
DIV	Direction pour l'immatriculation des véhicules
DPD	Délégué à la protection des données – Data Protection Officer (DPO)
DRI	Direction de l'information policière et des ressources τις
FEEDIS	Feeding information system (utilisé par la Police Fédérale)
GAFAM	Google, Apple, Facebook, Amazon, Microsoft
GPI	Geïntegreerde politie – Police intégrée
IA	Intelligence artificielle
ILP	Intelligence Led Policing (Police basée sur le renseignement)
ISLP	Integrated system for local police (Système intégré pour la police locale)
LDH	Ligue des droits humains (en Belgique francophone)
LEZ	Low Emission Zone (Zone à faibles émissions)
NACE	Nomenclature statistique des activités économiques dans la Communauté européenne
OSINT	Open-source intelligence (Recherche en sources ouvertes)
RGPD	Règlement général sur la protection des données
SICAD	Service d'information et de communication de l'arrondissement
TIC	Technologies de l'information et de la communication
ULB	Université libre de Bruxelles
VCA	Video content analysis (Analyse de contenu vidéo)
VUB	Vrije Universiteit Brussel

Photo de la quatrième de couverture : Commissariat central de Charleroi La Tour Bleue, conçue par Jean Nouvel CC-BY-Sa Corentin DebailleuL, 2023

