PETIT PAYS, BIG DATA

Automatisation de la discrimination et police "prédictive" en Belgique

Photo de couverture :
Commissariat central de la zone de police d'Anvers
CC-BY-SA 2.0 Fred Romero, 2016

PETIT PAYS, BIG DATA

Automatisation de la discrimination et police "prédictive" en Belgique

Avril 2025

STATEWATCH

LIGUE
DES DROITS
HUMAINS

LIGA
VOOR
MENSEN
RECHTEN

European
Artificial Intelligence
& Society Fund

TECHNOPOLICE.BE

tac
tiC

Table des matières

Méthodologie 9
Résumé 11
Introduction 17
I. Les initiatives locales en matière de police "prédictive" 20
1. Système d'information géographique (SIG) Orbit 20
2. Zone de police Westkust 21
3. Zone de police Zennevallei 23
4. Zone de police d'Anvers 27
II. Les bases de données policières en Belgique 30
1. Brève présentation des différents types de bases de données 30
a. La Banque Nationale Générale (BNG) 30
b. Les bases de données de base 31
c. Les bases de données particulières 32
d. La banque de données commune « Terrorisme, Extrémisme, Processus de Radicalisation » (BDC T.E.R.) 34
e. Les bases de données techniques 35
2. Les risques liés aux bases de données policières : études de cas 36
a. Base de données et profilage de travailleurs·euses du sexe 38
b. Bases de données et profilage des "bandes urbaines" (BU) 42
c. Discrimination à l'embauche, screenings et habilitations de sécurité 45
d. Screenings antiterroristes 48
e. Vers un droit d'accès direct ? 51
3. L'avenir des bases de données policières en Belgique 52
III. Le projet fédéral "i-Police" 53
1. Le "lac de données" i-Police 56
2. Vidéosurveillance 57
3. Recherche en sources ouvertes (OSINT), analyse algorithmique et sous-traitants 60
4. État d'avancement du programme "i-Police" 65
Automatisation de la justice en Belgique : petits pas, mais enjeux de taille 68
Conclusion : "Garbage In, Garbage Out" 69
1. Résumé 69
2. Discussion 71
Acronymes et abréviations 75

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.

https://creativecommons.org/licenses/by-sa/4.0/deed.fr

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

1 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.[2]

2 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.

« La police du 21ème siècle sera numérique ou ne sera pas »
Annelies Verlinden, ministre belge de l'Intérieur (2020-2025)[3]

Introduction

Les polices du monde entier comptent désormais sur les algorithmes pour analyser leurs bases de données ou profiler des coupables potentiels. La police dite "prédictive" s'est imposée comme un vecteur de transformation au sein des services de police à travers le monde, remodelant le paysage de la prévention et de la répression. Cette approche promet d'améliorer "l'efficience" et "l'efficacité" de la police en misant sur les algorithmes et les bases de données, marquant apparemment le début d'une nouvelle ère pour le maintien de l'ordre.

La police "prédictive" est une approche du maintien de l'ordre qui s'appuient sur l'analyse des données et les algorithmes d'apprentissage automatique (*machine learning*) pour "prédire" et ensuite chercher à "prévenir" de potentielles activités criminelles. Elle utilise les données de criminalité, ainsi que divers autres facteurs sociodémographiques et environnementaux, pour identifier des modèles et des tendances qui suggèrent *où*, *quand*, *par qui*, ou *sur qui*, un crime ou un délit est le plus susceptible de se produire.

Les principaux objectifs de la police "prédictive" sont d'allouer les ressources policières de manière plus efficace en anticipant et en devançant l'activité criminelle dans certains lieux ou zones ; de profiler des individus en tant que criminels (potentiels) afin de les surveiller de plus près ; voire de justifier des interventions policières telles qu'une interpellation, une fouille, un interrogatoire, ou une arrestation.

Cependant, le profilage et la police "prédictive" suscitent des inquiétudes quant à la partialité des données, et quant aux discriminations et aux violations potentielles des droits humains et des libertés publiques qui en découlent. La fiabilité de ces systèmes peut être mise en doute, en particulier lorsqu'ils sont fondés sur des théories pseudoscientifiques. La délimitation de "zones à risques" comporte également un risque de prophétie autoréalisatrice, lorsqu'une présence policière accrue dans certains quartiers est susceptible d'entraîner des interpellations et des fouilles, voire des arrestations. Les zones concernées ressortiront alors d'autant plus sur les cartes, ce qui incitera la police à les cibler de manière répétée, créant ainsi une boucle de rétroaction.

3 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.

Le même type de boucle risque de se former lorsque le ciblage de personnes issues d'un certain milieu ou correspondant à un profil particulier – souvent des personnes marginalisées ou racisées – pourra mener à des contrôles et des arrestations. Une fois inscrites dans les bases de données policières, ces nouvelles entrées conduiront potentiellement la police à cibler encore et encore les personnes correspondant à un profil particulier.

En outre, la question de la transparence se pose lorsque les algorithmes deviennent opaques et incompréhensibles, alors que la responsabilité est cruciale pour que les gens puissent remettre en question ces dispositifs et leurs résultats. Enfin, certains droits humains fondamentaux peuvent être menacés, notamment la présomption d'innocence ; le droit à la vie privée, à la libre circulation et à un procès équitable ; la liberté d'association et l'égalité de traitement devant la loi.[4]

La police "prédictive" en Belgique constitue un agencement complexe d'initiatives des agences fédérales et locales en charge du maintien de l'ordre. Ce rapport met en lumière les multiples facettes de la police "prédictive" en Belgique, en passant en revue les théories qui la sous-tendent, les technologies sur lesquelles elle repose et les implications sociales qu'elle dessine.

Ce rapport analyse un large corpus d'articles de presse, de communications publiques, de documents officiels, de questions parlementaires et de débats politiques. De plus, elle mobilise des rapports d'agences gouvernementales et d'organisations non gouvernementales, ainsi qu'un audit privé du département informatique de la Police Fédérale. Elle s'appuie également sur la littérature académique concernant la coproduction de systèmes de police "prédictifs" en Belgique. Par ailleurs des entretiens ont été menés avec des responsables de la police et des représentant·es d'associations impliquées dans la défense des droits humains ou auprès de groupes susceptibles d'être fichés par la police, tels que les groupes racisés ou les travailleuses·eurs du sexe. Des demandes d'accès aux documents administratifs ont également été introduites, cependant, les autorités policières ont eu recours à des exceptions légales pour limiter les informations fournies à ce qui était déjà disponible en sources ouvertes.

Le rapport est divisé en quatre sections. La première section couvre les capacités prédictives de la police et couvre les initiatives prises par les zones de police locales. La deuxième porte sur les différentes bases de données policières et décrit les différents risques associés à leur utilisation. La troisième partie est consacrée au programme "i-Police" de la Police Fédérale et à ses nombreuses ramifications. Enfin, le rapport se termine par un résumé de notre étude.

Ce rapport vise à aller au-delà de la simple observation de la technologie en action. À une époque où les données et les algorithmes dominent la prise de décision, notre objectif est d'exposer les défis et les risques posés par cette transformation. L'avenir de la police "prédictive" n'est pas prédestiné. Elle est influencée par les actions et les choix des individus, groupes, associations et élu·es. Il est de

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

notre responsabilité à tous de garantir que la voie à suivre soit synonyme de justice, d'équité et de protection des libertés fondamentales.

NB : L'utilisation de guillemets autour du terme "prédictif" dans ce rapport vise à rappeler que la police dite "prédictive" n'est pas réellement en mesure de prévoir les crimes et délits à venir. Elle souligne plutôt qu'elle est basée sur des algorithmes et des modèles statistiques permettant de dégager des probabilités et des tendances, plutôt que des prédictions définitives. Malgré les affirmations ou les espoirs des techno-évangélistes, les prophéties à la *Minority Report* relèvent toujours du domaine de la fiction.

I. Les initiatives locales en matière de police “prédictive”

En Belgique, la “police intégrée” (*geïntegreerde politie*, GPI) est structurée en deux niveaux : la Police Fédérale et 183 zones de police locale. Ces dernières prennent en charge la plupart des tâches attendues de la police administrative comme judiciaire, tandis que la Police Fédérale les appuie dans ces fonctions.

Plusieurs zones de police locale ont utilisé des systèmes géographiques de police “prédictive” et de profilage et ont participé à des programmes expérimentaux de police “prédictive” au cours des dernières années. La transparence relative à ce type d’initiatives est très limitée, il est donc possible que d’autres zones de police utilisent également des systèmes “prédictifs” et de profilage ou mènent d’autres projets similaires.

En 2020, des criminologues de la KU Leuven ont mené une enquête auprès des forces de police en Flandre et dans la région de Bruxelles-Capitale qui a révélé que près de la moitié des zones de police ayant répondu utilisaient une forme ou une autre d’analyse de données. Plus précisément, 43 % d’entre elles utilisaient une « analyse manuelle des données », tandis que 31 % avaient recours à une « analyse automatisée des données ».[5]

1. Système d’information géographique (SIG) Orbit

Le système d’information géographique (SIG) Orbit[6] est le principal outil utilisé dans les zones de police locales – dans près de cent d’entre elles à en croire la société.[7] Ce système permet de représenter dans l’espace les données historiques de criminalité et de délinquance, ce qui permet d’identifier de supposés “points chauds” (*hotspots)*.

Orbit propose des outils permettant de représenter des faits de cambriolage, de vol à l’étalage, de stupéfiants, de nuisance et de vandalisme, par exemple « commis par des mineurs autour d’un nouveau chantier ».[8] Il propose également d’autres outils pour la « visualisation en temps réel » de « tous les effectifs et plans d’action d’événements en un seul écran », ainsi qu’un outil spécifique pour la “gestion négociée de l’espace public”.[9]

5 Lore Rooseleers et 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

6 Orbit GIS. *Zones de police*. URL: web.archive.org/web/20230930192819/https://www.orbitgis.com/fr/zone-de-police
La société a été renommée “Columba” en 2024. URL: www.columbasoftware.be/software/veiligheidsdiensten

7 Orbit GIS. *Zones de police.* url: www.orbitgis.com/fr/zone-de-police

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

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

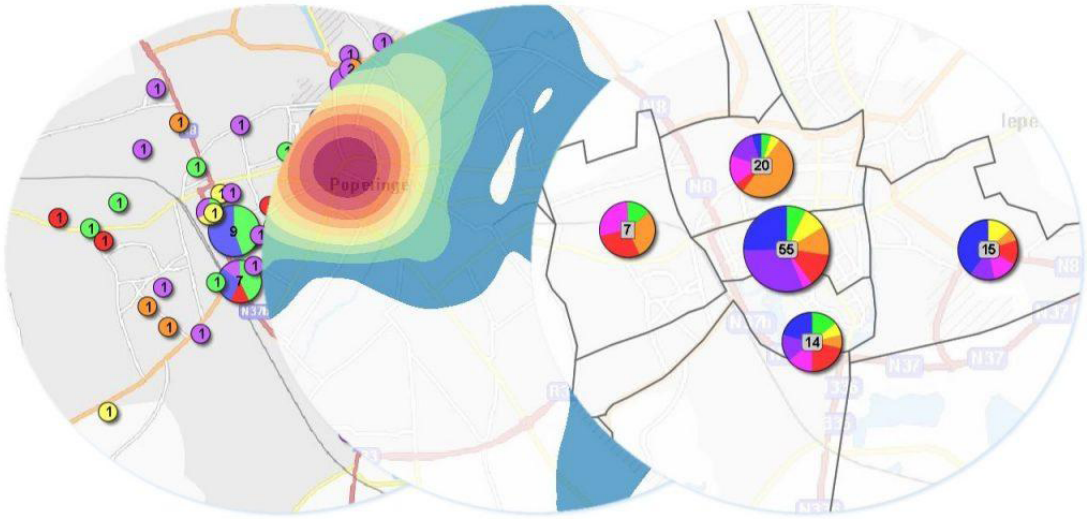

Figure 1. Capture d'écran du site web d'Orbit
URL: www.orbitgis.com/fr/zone-de-police/zp_strategie

Nombre d'études ont cependant montré que la focalisation sur les "points chauds" tend à perpétuer des pratiques discriminatoires, en particulier par une surveillance et une répression accrue de certains quartiers ou de certaines personnes.[10] En effet, plus la police patrouillera dans certaines zones et contrôlera certains profils (en délaissant d'autres profils), plus elle pourra construire un biais de confirmation. Cela n'empêche pas plusieurs zones de police flamandes d'avoir entrepris des essais pilotes de police "prédictive", sur lesquels ce rapport se concentre à présent.

2. Zone de police Westkust

La zone de police Westkust couvre les communes flamandes de La Panne, Coxyde et Nieuport. Il s'agit de communes limitrophes de la France, à l'ouest de la côte belge. Seules 45 000 personnes y habitent, mais la région attire de nombreux touristes en période de vacances.

Figure 2. Photo panoramique de la plage de La Panne
Copyleft Lokilech, 2008.

10 William Isaac et Kristian Lum, 'To Predict and serve?', *Royal Statistical Society*, 2016, DOI: 10.1111/j.1740-9713.2016.00960.x; Lyria Bennett Moses et 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 et 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

La zone de police Westkust a été précurseure du processus de numérisation de la police, en se lançant dans la course de la police "prédictive" dès 2016.[11] Nicholas Paelinck, le commissaire principal local, s'est personnellement rendu à Philadelphie, aux États-Unis, pour observer comment la police y déployait déjà de tels systèmes et pour voir comment ceux-ci pourraient être importés dans la zone de police Westkust.

L'objectif déclaré de la zone de police est d'avoir « moins de bleu dans les rues », c'est-à-dire moins de patrouilles mais plus d'analystes de données.[12] S'adressant à la presse, le commissaire principal a expliqué comment le projet était censé fonctionner :

> Nous travaillons déjà avec trois gestionnaires de données au sein de notre corps. Grâce aux informations qu'ils reçoivent, nous prévoyons grosso modo où les choses pourraient mal tourner. Nous y envoyons alors une équipe d'intervention de manière proactive. Il ne s'agit pas seulement de prévenir les cambriolages, mais le modus operandi sert aussi à des actions préventives contre les voleurs d'armes ou les trafiquants de drogue. L'idée est de s'attaquer à la criminalité avant que les faits ne se produisent.[13]

Le fonctionnement réel du programme n'a été décrit qu'en termes généraux :

> La police recueille un grand nombre de données différentes, allant des crimes passés aux plaques d'immatriculation, en passant par les dossiers judiciaires et même la météo, qui sont introduites dans l'ordinateur. À l'aide d'algorithmes, les analystes de données évaluent exactement où et quand les crimes pourraient se produire dans un avenir proche.[14]

Le commissaire principal estime que, depuis l'introduction du programme, les incidents criminels ont diminué de 40 %. La police affirme que les capacités "prédictives" du logiciel sont particulièrement efficaces pour lutter contre les cambriolages et les vols de véhicules.[15] Toutefois, la fiabilité de ces statistiques – non étayées – doit être remise en question. Aucune évaluation objective du système n'est accessible au public et les informations concernant le programme informatique utilisé pour effectuer l'analyse et les prévisions ou l'affectation des fonds n'ont jamais été divulguées.

Au fur et à mesure de l'évolution du système, le commissaire entend intégrer au logiciel les caméras de reconnaissance automatique des plaques d'immatriculation (ANPR).[16]

---

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

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

13 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/

14 Haco. "Politiezone Westkust experimenteert met datasets in strijd tegen criminaliteit". *Op. Cit.*

15 *Ibid.*

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

Par ailleurs, le commissaire principal de la zone Westkust est également le président du Comité permanent de la police locale (CPPL), l'organisation qui chapeaute les zones de police locale. Il est donc bien placé pour diffuser les techniques de police "prédictive" expérimentées sur la côte vers les zones de police de tout le pays.[17]

3. Zone de police Zennevallei

La zone de police Zennevallei couvre les municipalités de Beersel, Hal et Leeuw-Saint-Pierre dans la banlieue flamande au sud-ouest de Bruxelles. En 2020, la zone a lancé un projet de collaboration de deux ans avec l'Université de Gand, axé sur le concept de "police prédictive". La zone de police prétend élaborer des "prédictions" sur les lieux qui présenteraient un risque accru d'activités criminelles, comme des cambriolages ou d'autres délits.[18]

Figure 3. Vue aérienne de la Chaussée de Mons à Leeuw-Saint-Pierre
CC-BY-SA 3.0 Wouters Hagens, 2014

À l'occasion d'une remise de prix en 2022, un communiqué annonçait :

> La zone de police Zennevallei, en collaboration avec l'UGent, a lancé en octobre 2019 un projet pour développer et tester un modèle de gestion policière basé sur les données massives (*big data*). Le projet s'est principalement concentré sur les cambriolage de domiciles, soit le délit le plus courant en Belgique et qui a un impact psychologique majeur sur les victimes. Le projet a été concrétisé entre 2020 et 2021. Ainsi, des cartes de risques ont été établies sur base de modèles statistiques

17 CPPL, 2019. *Memorandum 2019-2023*. Commission Permanente de la Police Locale. pp. 5 ; 44-45. URL: www.police.be/5806/sites/5806/files/downloads/Memorandum%20FR_0.pdf
18 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

> alimentés par des données massives, qui ont ensuite été utilisées pour orienter de manière proactive les patrouilles de police. À court terme, cela a permis d'obtenir des évaluations de risques indiquant la probabilité de la criminalité. Les personnes et les ressources ont pu être déployées en conséquence dans ces zones à haut risque. À long terme, nous voulions être en mesure d'utiliser les ressources policières plus efficacement et de réduire la criminalité.[19]

Le système de police "prédictive" de la zone de police Zennevallei a attiré l'attention du Sénat, qui a interpellé le gouvernement à ce sujet. En réponse, la ministre de l'Intérieur a indiqué qu'elle soutenait les efforts de la police pour améliorer ses capacités d'analyse et a souligné l'importance fondamentale d'établir une base solide pour la police "prédictive", y compris par l'acquisition des données nécessaires. Toutefois, la ministre de l'Intérieur a également reconnu que les statistiques policières « reflètent avant toute chose l'activité policière » et non « la réalité criminelle d'un territoire donné ».[20]

Le projet de la Zennevallei a été mené par Anneleen Rummens, alors doctorante à l'université de Gand, sous la supervision du professeur de criminologie Wim Hardyns. Ils ont recueilli des données massives (*big data*) sur la criminalité locale reprenant nombre de variables. Celles-ci comprenaient le lieu et l'heure d'incidents, ainsi que des facteurs contextuels tels que les conditions météorologiques, avec pour objectif de cartographier toutes ces informations.[21]

Leur méthode est basée sur la modélisation de "zones à risque" (*Risk Terrain Modelling* – RTM), une méthode de police "prédictive" qui s'appuie sur la criminologie et les systèmes d'information géographique (SIG) pour tenter d'identifier les quartiers potentiellement plus exposés aux activités criminelles. La RTM repose sur l'idée que des facteurs environnementaux particuliers définissent des "zones à risque" où les crimes et délits sont plus fréquents.

Cependant, la RTM fait l'objet de nombreuses critiques en raison des théories criminologiques qui la sous-tendent.[22] En effet, le principe fondamental au cœur de la RTM est que certaines zones géographiques attirent ou génèrent intrinsèquement des activités criminelles.[23] Or, cette hypothèse est loin d'être étayée scientifiquement, dans la mesure où les causes de la criminalité et de la délinquance sont plutôt à chercher dans une interaction complexe entre divers facteurs sociaux, économiques et individuels. En mettant l'accent sur la dimension "environnementale", on néglige les facteurs socioéconomiques et structurels sous-jacents de la criminalité.

---

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

20 Réponse de la ministre de l'Intérieur du 09/07/2020 à la question écrite n°7-591. *Sénat de Belgique*. URL: senate.be/www/?MIval=/Vragen/SVPrintNLFR&LEG=7&NR=591

21 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, n° 4, pp. 1035–1053. DOI: 10.1007/s12061-020-09339-2

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

23 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

Les criminologues de Gand prétendent s'affranchir de ces critiques en intégrant des facteurs socioéconomiques parmi leurs critères. Leur modèle inclut donc des variables telles que les pourcentages de jeunes et d'immigrés, ou la densité de logements sociaux et de snacks.[24] Loin de lutter contre les causes structurelles de la criminalité, ces cartographies peuvent renforcer les discriminations en ciblant de manière disproportionnée certains quartiers. Cela peut perpétuer des pratiques déjà à l'œuvre, ciblant les quartiers défavorisés et exacerbant les inégalités existantes. Comme l'explique le géographe Brian Jefferson :

> La manière dont les préjugés de la police et de la Justice affectent les statistiques de criminalité n'est pas systématiquement explorée par ces approches. Elles n'abordent pas non plus la façon dont les lois, les politiques ou les pratiques policières influencent les données de criminalité et leur géographie. Les cartes de criminalité n'offrent pas tant des images définitives et objectives des comportements illégaux, mais soulèvent plutôt des questions sur la manière dont ces comportements sont enregistrés et étudiés.[25]

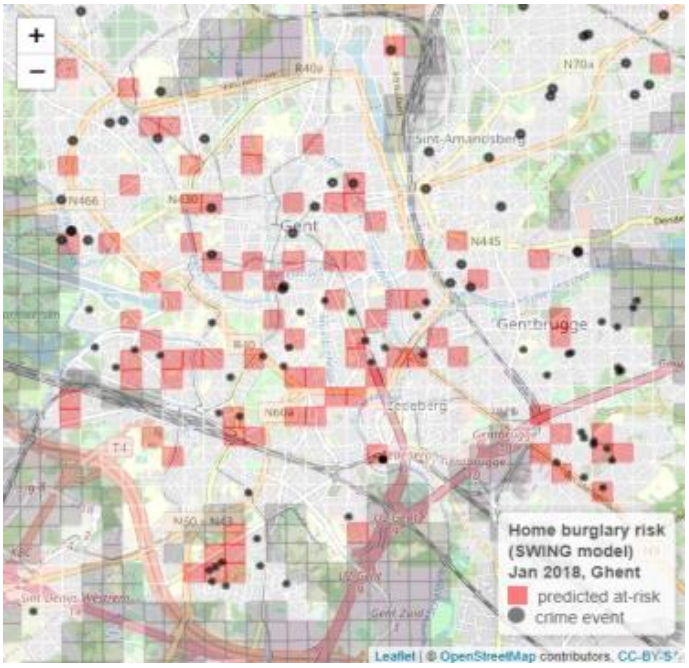

Figure 4. Cambriolages prédits (carrés rouges) et cambriolages réels (points noirs) à Gand
Source : Rummens & Hardyns. CPS international conference "Street policing in a smart society". 17/09/2019.

Hardyns et Rummens ne semblent guère se préoccuper des conséquences du système qu'il et elle ont mis au point en matière de discrimination, compte tenu notamment de l'abondance des données sensibles en jeu. Lors d'une conférence, Hardyns a tenté d'éteindre les inquiétudes liées aux discriminations en invoquant la prétendue neutralité de la technologie. Pour illustrer sa supposée neutralité, Hardyns affirme que « les armes ne tuent pas les gens. Ce sont les gens stupides et armés qui tuent les gens ».[26] L'argument de la neutralité technologique est le suivant : la technologie ne serait pas intrinsèquement bonne ou mauvaise ; au

24 Anneleen Rummens & Wim Hardyns. 2020. "Comparison…". *Op. Cit.*, Table 2.
25 Brian Jefferson. 2020. "Crime Mapping", *Op. Cit.*, p. 14.
26 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

contraire, sa valeur éthique dépendrait de son utilisation. Cet argument est toutefois facilement réfutable. Le potentiel de nuisance d'une technologie est en réalité largement déterminé par ses caractéristiques techniques, car sa production est intrinsèquement liée à son contexte social et à ses objectifs.

À l'issue de leur recherche, les chercheurs Hardyns et Rummens de l'université de Gand sont parvenus à la conclusion suivante :

> La police prédictive peut permettre une utilisation plus ciblée des données afin de mettre en place un fonctionnement basé sur les données au sein des forces de police. Outre les nouvelles sources de données, la mise en œuvre de nouvelles méthodes telles que l'apprentissage automatique peut fournir des informations dynamiques sur l'évolution des schémas de criminalité. Néanmoins, de nombreuses sources de données et méthodes connexes restent largement inexplorées. Par exemple, les données des médias sociaux et les nouvelles méthodes dans le vaste domaine de l'apprentissage automatique (par exemple, les modèles d'apprentissage profond, la version avancée des réseaux neuronaux) pourraient être envisagés. À l'heure actuelle, le potentiel d'exploration de ces nouvelles sources et méthodes n'a pas encore été exploité.[27]

Récemment, l'équipe de Hardyns a également tenté d'identifier des tendances dans les statistiques de criminalité à Bruxelles. En présentant les résultats de leurs recherches, ils formulent également une série de recommandations qui rejoignent l'engouement pour la police "prédictive", appelant à davantage de données massives et d'automatisation, ainsi qu'à l'intégration de multiples sources de données :

> La criminalité à Bruxelles est davantage liée à la mobilité des délinquants et criminels, et nécessite donc peut-être des approches axées sur ceux-ci visant à suivre leurs déplacements en temps réel, par exemple en utilisant des lecteurs automatiques de plaques d'immatriculation (LAPI [ou ANPR]) ou des systèmes de surveillance. D'une manière générale, il pourrait donc être utile de suivre et d'analyser régulièrement les données relatives à la criminalité et donc de mettre en œuvre une approche policière guidée par le renseignement en temps réel. À cet égard, il pourrait également être recommandé de combiner les approches policières basées sur le lieu et sur la personne ou d'appliquer des approches plus dynamiques qui prendraient en compte le niveau de concentration de la criminalité, l'(in)stabilité spatiale de la criminalité, la mobilité des délinquants et criminels, et les informations en temps réel (par exemple, les approches policières prédictives basées sur le lieu). [...]
>
> En outre, il est crucial d'explorer l'intégration potentielle d'autres sources de données massives avec les registres officiels de police. L'intégration d'informations pertinentes provenant de sources telles que les médias sociaux (par exemple, les données de Twitter) et l'utilisation de techniques d'exploration de texte peuvent fournir des informations qualitatives sur les incidents liés à la criminalité. Cela pourrait enrichir notre compréhension des concentrations de criminalité et contribuer à des analyses plus complètes et innovantes.[28]

27 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

28 Robin Khalfa, Thom Snaphaan, Lieven Pauwels, Ourania Kounadi & Wim Hardyns, 2023. "Crime with-

Compte tenu de la place de Hardyns dans le développement de modèles "prédictifs" pour le compte de la police, il sera tout indiqué de suivre les futures recherches menées sous sa direction. En 2023, il s'est vu attribuer près de 2 millions d'euros par l'UE pour mener, durant cinq ans, un projet appelé bigdatpol.[29] L'objectif de cette recherche est « d'intégrer les conditions statistiques, méthodologiques, criminologiques, juridiques et éthiques dans un modèle 3D unique fondé sur des faits » devant fournir « à la fois au monde universitaire et policier des lignes directrices et des recommandations pour étudier, appliquer et assurer le maintien de l'ordre fondé sur les données massives ».[30] Pas moins de vingt zones de police flamandes ont accepté de participer à cette recherche.[31] Enfin, Hardyns et son équipe ont également travaillé sur la ville d'Anvers, dont il est question ci-dessous.

4. Zone de police d'Anvers

Anvers est la deuxième plus grande ville de Belgique, mais ne compte qu'une seule zone de police, alors que Bruxelles, la capitale, est divisée en six zones distinctes. La zone de police locale d'Anvers est donc l'une des zones les plus importantes du pays. Cette situation est accentuée par le fait que la police locale dépend de l'administration locale, dirigée de 2013 à 2025 par Bart De Wever (2013-2025), chef de file des nationalistes flamands et nommé Premier Ministre belge en février 2025.

Figure 5. Les abords de l'Escaut à Anvers
CC-BY-SA 3.0 Paul Hermans, 2012

in 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.

29 "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

30 '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

31 BIGDATPOL. 'Kick-off field test Belgium'. *nwsltr*. n°1. Summer 2024. URL: bigdatpol.com/wp-content/uploads/2024/08/SUMMER-2024-NWSLTR_LR.pdf

L'influence de la zone de police d'Anvers sur la numérisation et l'automatisation du maintien de l'ordre en Belgique s'illustre par un certain nombre de marchés publics conclus par la police locale d'Anvers et étendus par la suite à d'autres zones de police du pays.

Anvers a signé un contrat de 2 000 000 € avec l'entreprise suédoise Securitas[32] pour la privatisation de certaines fonctions policières telles que la surveillance d'événements publics et de zones stratégiques, ou le visionnage des images de vidéosurveillance.[33] Le même contrat permet également l'achat d'équipements, et de nombreuses zones de police belges y ont recours pour acheter des caméras-piétons (*bodycams*).

De plus, la police d'Anvers a développé sa propre application pour smartphone, appelée FOCUS, qui permet aux policiers d'accéder aux bases de données policières. Anvers a ensuite vendu l'application à la police intégrée pour la déployer dans tout le pays.

L'offre standard de FOCUS, accessible à chaque zone de police belge, se compose de plusieurs modules :

Le module "Recherche" permet aux agents d'explorer toutes les bases de données disponibles. Le module fournit des informations de manière proactive. Lorsque les agents introduisent un lieu, il récupère automatiquement des données sur les personnes (et éventuellement les armes) enregistrées à cette adresse, ainsi que sur les incidents passés ;

- Le module "Incidents" fournit aux policiers·ères une vue d'ensemble des événements en cours sur le terrain ;
- Le module "ISLP" (*Integrated System for the Local Police*) permet aux policiers de créer rapidement des rapports sur le terrain ;
- Le module "Messages" offre une plateforme de communication aux policiers·ères ;
- Le module "Images" permet de prendre des photos ;
- Le module "Maps" comprend plusieurs couches de cartes, y compris la localisation des unités, des caméras de surveillance et un aperçu de la circulation.

Les zones de police ont par ailleurs la possibilité d'enrichir l'application FOCUS avec des modules supplémentaires, notamment pour les contrôles domiciliaires.[34]

Un algorithme développé pour être intégré dans le système FOCUS permet à la police de rassembler des données provenant de diverses sources, notamment la base de données principale de la police (BNG), des caméras anpr et le registre des plaques d'immatriculation (DIV), ainsi que le "système intégré pour la police locale" (ISLP).

32 Securitas Security company. URL: www.securitas.be

33 Lokale Politie Antwerpen. LPA/2017/295. URL: enot.publicprocurement.be/enot-war/preViewNotice.do?noticeId=319270

34 Lore Rooseleers & Jeroen Maesschalk. 2021. "Digitalisering in de lokale politie in Vlaanderen en Brussel: Waar staan we?" *Op. Cit.*

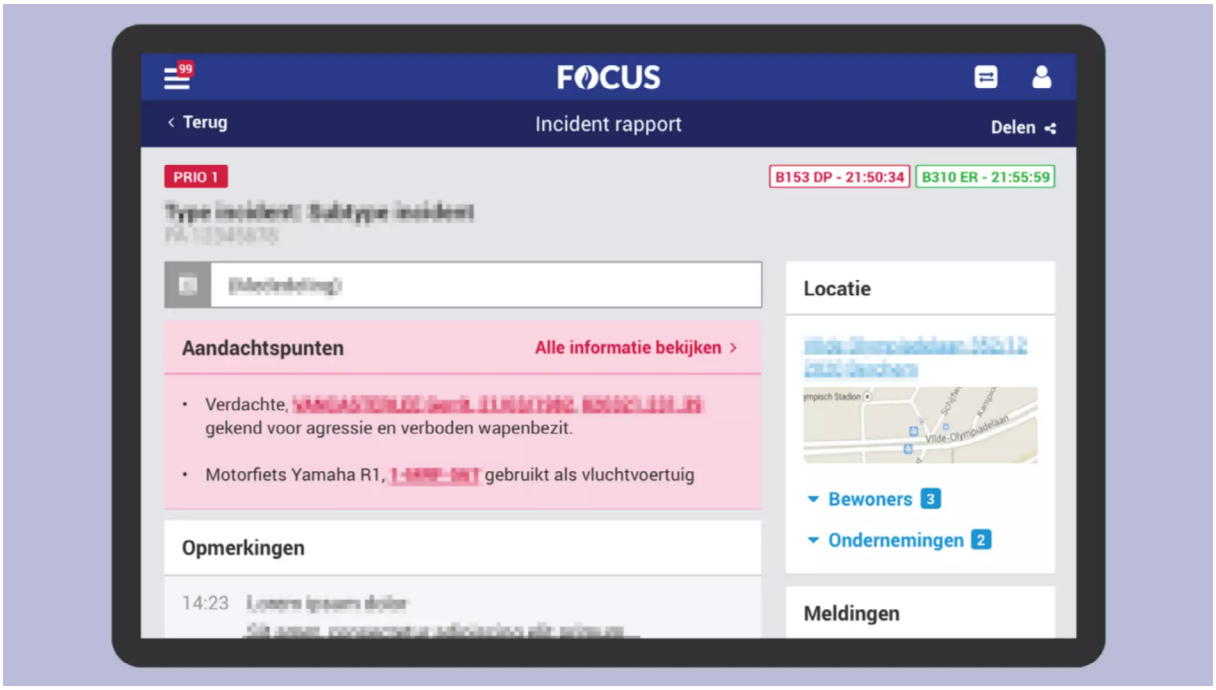

Figure 6. L'interface utilisateur de l'application FOCUS
Source: Monkeyshot. 2018. "A typical user research for the Antwerp police force – IxD18". *Slideshare.*

L'utilisation des données issues d'ISLP pose un problème particulier car ces informations ne sont pas vérifiées et consistent principalement en des notes de terrain non corroborées, en ce compris des opinions et des rumeurs.

En outre, une autre plateforme logicielle a été mise en place à Anvers, regroupant des images de caméras de surveillance, des données ANPR, les localisations des voitures de police, ou encore des données liées à la gestion de foule par le suivi des téléphones portables. Par ailleurs, des techniques d'analyse ont également été appliquées aux images de vidéosurveillance telles que la reconnaissance de texte, le suivi d'objets, le "parsage" humain[35] ou le profilage comportemental.[36]

A l'avenir, Jo Forceville, spécialiste en *smart policing* de la police d'Anvers, prévoit une transition vers des méthodes basées sur l'intelligence artificielle (IA) et la recherche en sources ouvertes (OSINT) :

> Des projets sont en cours sur l'exploration (*scraping*) des réseaux sociaux, les modèles d'apprentissage en profondeur (*deep learning*) et l'utilisation de l'IA dans l'analyse des images des caméras. L'exploration des réseaux sociaux est utilisée dans les enquêtes sur le radicalisme, par exemple pour rechercher des schémas ou des itinéraires suspects dans la circulation.[37]

Il est clair que la zone de police d'Anvers est à la pointe de l'utilisation des nouvelles technologies. Qui s'intéresse au futur de la police belge devra surveiller l'évolution de la ville portuaire flamande.

35 Soit la segmentation d'une image humaine en différentes parties signifiantes comme la tête, le corps, les bras ou les jambes.
36 Jo Forceville. 2023. "Big Data en politie, evolutie in versnelling: Een blik voorbij data en technologie". In Snaphaan *et al. (eds.). Cahiers Politiestudies. n° 66: Big Data Policing. Antwerpen: Gompel&Svacina. pp. 107-120.*
37 *Ibid.*

II. Les bases de données policières en Belgique

Les bases de données policières serviront de source principale pour les systèmes de police “prédictive” et de profilage par les données. Il est donc important de les présenter brièvement.

Les bases de données policières belges sont officiellement divisées en cinq catégories :

a) La banque nationale générale (BNG) ;

b) Les bases de données de base ;

c) Les bases de données particulières ;

d) La base de données commune (BDC) ;

e) Les bases de données techniques.

Les sources de données privées, notamment les réseaux sociaux et les données de géolocalisation fournies par les opérateurs téléphoniques,[38] jouent également un rôle important et seront abordées plus en détail ultérieurement.

1. Brève présentation des différents types de bases de données

a. La Banque Nationale Générale (BNG)

La Banque Nationale Générale (BNG) est la principale base de données de la police et est divisée en trois sections : la police de la route, la police administrative et la police judiciaire. Dans la pratique, cette base de données est fréquemment consultée dans le cadre de diverses enquêtes policières. La BNG contenait en 2019 des informations sur pas moins de trois millions de personnes, soit un quart de la population belge.[39] La fiabilité de ces informations est variable et peut concerner tant des suspects, que des témoins ou victimes, et ce quel que soit le type d’incident. Depuis 2019, les mesures répressives liées à la pandémie de Covid n’ont certainement pas fait diminuer ce chiffre.

38 Corentin Debailleul. 2021. “Pistage dans le cyberespace”. *Culture & Démocratie*. n° 53. URL: www.cultureetdemocratie.be/articles/pistage-dans-le-cyberespace/

39 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/

L'organe de contrôle de l'information policière (COC) a récemment publié un rapport caustique sur l'utilisation de la BNG.[40] Le protocole officiel stipule que les données non vérifiées doivent être contrôlées par une seconde partie avant d'être intégrées dans la BNG. Cependant, il arrive régulièrement que des informations douteuses soient intégrées dans la base de données.

Les requêtes dans les bases de données policières sont entourées d'une culture de légitimité présumée et les officiers qui ne respectent pas le protocole bénéficient d'une certaine indulgence. Ce n'est que récemment que la police a mis en place des procédures d'archivage pour supprimer les données obsolètes, ce qu'elle est légalement tenue de faire[41]. Comme c'est souvent le cas lorsque la police s'écarte de la voie légale, les sanctions sont faibles, voire inexistantes. C'est ainsi que le directeur du COC explique la situation :

En tant que membre du Comité P [Comité permanent de contrôle des services de police] en 2007 ou 2008, j'ai fait une étude, une analyse de toutes les sanctions, tous les jugements vis-à-vis des fonctionnaires de police et il s'est avéré de façon manifeste que les fonctionnaires de police sont en fait jugés de façon très légère, [...] bien souvent on ne fait pas de poursuites.[42]

Catherine Forget, avocate et chercheuse en droit, a observé que « la BNG archive les données pendant trente ans avant de les supprimer. Toutefois, il convient de noter qu'en principe, les données traitées dans les bases de données policières et judiciaires doivent être archivées lorsqu'elles sont jugées inadéquates, non pertinentes ou excessives, indépendamment des délais de conservation. »[43]

Dans la pratique cependant, les périodes de conservation des données sont souvent largement dépassées, ce qui entraîne le stockage indéfini de données sans archivage ni suppression.[44] Par exemple, l'actuel délégué à la protection des données (DPD) de la zone de police de Charleroi a déclaré qu'à sa nomination en 2014, il a été confronté à des milliers de procédures inachevées dans la BNG qui devaient être terminées. Il a fallu plusieurs années pour éliminer l'arriéré.[45]

b. Les bases de données de base

Les bases de données de base enregistrent essentiellement les notes prises sur le terrain par les policiers au cours de leurs opérations. Les bases de données de base sont utilisées par la police intégrée et couvrent les données traitées à des fins de police administrative et judiciaire, y compris les procès-verbaux et les rapports relatifs à des événements spécifiques – ce qui peut englober un large éventail de situations.

40 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.organedecontrole.be/files/DIO23001_F.pdf
41 COC, 2023. DIO23001. *Op. Cit.*
42 Audition du COC au Parlement Fédéral suite au rapport sur la BNG. 28/06/2023. *Chambre des représentants de Belgique*. Doc 55 3467/001.
43 Catherine Forget. "L'effacement des données policières et judiciaires : un parcours du combattant ?". *e-legal, Revue de droit et de criminologie de l'ULB*, n°6, mars 2022.
44 *Ibid.*
45 Entretien avec le DPD de la zone de police de Charleroi. 03/07/2023.

La BNG est alimentée par les enregistrements des bases de données de base. Cela se fait au moyen d'applications telles que ISLP (*Information System for the Local Police*), qui sert à encoder les procès-verbaux ; FEEDIS (*Feeding Information System*) pour la Police Fédérale ; et GES/Itinera, qui « offre à tous les services d'enquête fédéraux la possibilité de consulter, presque en temps réel, l'état d'avancement de leurs dossiers auprès du département de la Justice ».[46]

c. Les bases de données particulières

Les bases de données particulières sont mises en place pour répondre à des besoins spécifiques. D'après la loi sur la fonction de police :

> Dans des circonstances spécifiques, les chefs de corps, le commissaire général, les directeurs généraux et les directeurs peuvent créer, pour des besoins particuliers, des banques de données particulières dont ils sont responsables du traitement, dans le but de traiter les données qu'elles contiennent dans le cadre de l'exercice de leurs missions et finalités de police administrative et judiciaire.[47]

Elles sont créées et conservées au sein des services de police pour des besoins spécifiques. Pour quels besoins exactement ? Le directeur du COC nous éclaire :

> Il peut s'agir de n'importe quoi. Par exemple, les bandes de jeunes, il y en a certainement en région bruxelloise. Il y a six zones de police locales dans la région de Bruxelles et probablement toutes ont une base de données sur les bandes de jeunes ou ont une base de données sur le terrorisme et/ou la radicalisation. Il s'agit donc, par exemple, de personnes connues pour des cambriolages, de récidivistes. Ce sont toutes des options possibles lorsqu'il s'agit de bases de données particulières.[48]

Ces bases de données sont fréquemment utilisées au niveau local, mais la Police Fédérale y a également recours. Par exemple, la branche administrative de la Police Fédérale est responsable de la supervision des manifestations et utilise des bases de données particulières pour les activistes supposément d'extrême droite ou d'extrême gauche.[49]

Beaucoup de ces bases de données particulières existent sous les radars, hors de la surveillance du COC, qui a déclaré :

Je pense qu'il y a environ 1600 de ces bases de données dont nous avons connaissance. Mais je ne connais évidemment pas tout. En principe, il n'existe pas de système d'accès direct, et certainement pas d'accès direct à des bases de données particulières. Mais ici, c'est en fin de compte le chef de la police locale qui décide qui peut y avoir accès ou non. [...] C'est la grande différence entre les trois types de bases de données. Pour les bases de données de base et la BNG, les ministres de l'Intérieur et de la Justice sont responsables de traitement, mais pour les bases de

46 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

47 Art. 44/11/3 de la loi sur la fonction de police du 5 août 1992. URL: ejustice.just.fgov.be/eli/loi/1992/08/05/1992000606/justel

48 Entretien avec Frank Schuermans (COC), 17/02/2023.

49 Entretien avec des délégués syndicaux de la Police Fédérale, 17/08/2023.

données locales, pour ces bases de données particulières, c'est le chef de la police locale qui décide. [...] Pour nous, il est donc évidemment beaucoup plus compliqué d'avoir une bonne vue d'ensemble de ces bases de données particulières. Il n'y a qu'une seule façon de savoir, c'est de s'adresser à la police locale et de lui demander de nous montrer ce qu'il en est.[50]

Le COC a aussi critiqué le manque de contrôle des bases de données particulières :

> En ce qui concerne les bases de données particulières, je pense que c'est un vrai problème parce que la plupart d'entre elles ne sont pas journalisées (*logged*). Les zones de police qui veulent faire les choses correctement, essaient de le faire au fur et à mesure. Les systèmes sont très spécifiques et il peut s'agir d'un simple fichier Excel, de sorte que les procédures d'authentification sont très différentes, mais pour nous ce sera un gros problème à l'avenir, il est donc important de mettre de l'ordre, et il y a du boulot ![51]

En ce qui concerne la possibilité d'utiliser ces bases de données, le COC est tout à fait explicite :

> Lorsque nous effectuons des audits proactifs, nous demandons toujours de nous fournir une liste de toutes les bases de données particulières et de nous expliquer pourquoi il est nécessaire de disposer de cette base de données. Dans 99 % des cas, lorsque nous arrivons avec, par exemple, 25 à 30 bases de données particulières, la moitié d'entre elles ont disparu lorsque nous quittons les lieux ou lorsque notre enquête est terminée.[52]

Ce point de vue nous a également été confirmé par le délégué à la protection des données (DPD) de la zone de police de Charleroi. Sans surprise, celui-ci estime que la BNG présente plusieurs avantages : elle est accessible aux autres services de police, elle est mieux régie et contrôlée, et ses données doivent être validées. Il affirme que les bases de données particulières ne sont utiles que dans des cas exceptionnels. Par exemple, la BNG ne permet pas de télécharger des images en haute définition. Dans l'ensemble, le DPD de la zone de police de Charleroi considère toutefois la BNG comme l'option privilégiée.

Du point de vue des droits humains, la question est faussée car les deux formes de bases de données policières présentent des risques considérables. Choisir entre une BNG pleine à craquer et des bases de données locales mal gérées revient à choisir entre la peste et le choléra. Nous y reviendrons dans une section ultérieure.

50 Entretien avec Frank Schuermans (COC), 17/02/2023.
51 Audition du COC au Parlement Fédéral suite au rapport sur la BNG. 28/06/2023. *Op. Cit.*
52 Entretien avec Frank Schuermans (COC), 17/02/2023.

d. La banque de données commune « Terrorisme, Extrémisme, Processus de Radicalisation » (BDC T.E.R.)

La BDC T.E.R. permet à la police et aux services de renseignement de partager des informations, en particulier dans le cadre de la lutte contre le « terrorisme, l'extrémisme et les processus de radicalisation ».[53] Selon l'opérateur de la base de données, l'Organe de Coordination pour l'Analyse de la Menace (OCAM), le dénominateur commun de tous les individus inclus dans la bdc est la violence, avérée ou potentielle.

La banque de données commune contient cinq catégories, définies comme suit :

- Foreign Terrorist Fighters (FTF) : personnes qui sont parties vers une zone de conflit dans le but de se rallier à un groupe terroriste, ou qui en reviennent, ainsi que les personnes qui ont été empêchées de partir ou qui ont l'intention de le faire ;

- Homegrown Terrorist Fighters (HTF) : personnes qui n'ont pas l'intention de partir pour rejoindre une organisation terroriste à l'étranger, mais qui choisissent de commettre des actions terroristes en Belgique ou qui offrent leur soutien à celles-ci ;

- Propagandistes de la haine (PH) : personnes voulant justifier le recours à la violence à des fins idéologiques, ainsi qu'exercer une influence radicalisante sur leur entourage et nuire à l'État de droit ;

- Extrémistes potentiellement violents (EPV) : personnes avec des conceptions extrémistes qui ont une intention de recourir à la violence, sans pour autant avoir entrepris des démarches concrètes à cette fin ;

- Personnes condamnées pour terrorisme (PCT) : personnes condamnées, internées ou faisant l'objet d'une mesure de protection pour terrorisme en Belgique ou à l'étranger.[54]

Si certaines catégories sont clairement définies, d'autres sont largement ouvertes à l'interprétation. Le comité de vigilance en matière de lutte contre le terrorisme (Comité T) dénonce à ce sujet l'élargissement progressif de la BDC T.E.R. à des catégories toujours plus larges et toujours plus floues.[55] Cela est d'autant plus problématique que cette base peut être utilisée pour accorder ou refuser des habilitations de sécurité.[56]

53 "La Banque de données commune (BDC)". *OCAM*. URL: ocam.belgium.be/la-banque-de-donnees-commune-bdc/

54 *Ibid.*

55 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

56 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

En 2022, la BDC T.E.R. comptait environ 700 personnes. Les autorités affirment que 87 % d'entre elles « adhèrent à une idéologie djihadiste », 10 % seraient liées à l'extrême droite et 2 % à l'extrême gauche. Les quelques cas résiduels figurent dans la banque en raison de « diverses menaces » trouvant leur source dans des « sentiments anti-establishment nés de la pandémie de Covid-19 ou un contexte politique à l'étranger ».[57]

e. Les bases de données techniques

La dernière catégorie de banques de données policières, les bases de données dites "techniques", se distinguent des autres en ce qu'elles contiennent des données et des informations personnelles collectées automatiquement – à l'heure actuelle, exclusivement par le biais de caméras de reconnaissance automatique des plaques d'immatriculation (ANPR) qui disposent d'un accès direct à la base de données nationale des véhicules (DIV), ce qui permet d'identifier des véhicules spécifiques présentant un intérêt, tels que les voitures volées ou non assurées.

Le COC a récemment déclaré relativement aux ANPR : « nous ne pouvons pas savoir qui a consulté ces données et à quel moment, il n'y a pas de registre, ce qui pose un problème juridique ».[58] Ce qui est un euphémisme pour dire que c'est proprement illégal.[59]

Figure 7. Une caméra ANPR de la marque Macq (à gauche) et des panneaux officiels (à droite), à Saint-Gilles, en région de Bruxelles-Capitale
Photos de Corentin Debailleul, CC-BY-SA.

Justifiées par un éventail de raisons allant de l'antiterrorisme à la mise en place de zones à faibles émissions (*Low Emission Zone* – LEZ), les caméras ANPR jouent un rôle important dans les efforts de surveillance belges. L'ambiguïté de leur objectif suscite des inquiétudes quant au détournement d'usages (*function creep*), c'est-à-dire l'expansion d'une technologie au-delà de ses objectifs initiaux.

57 "700 extrémistes font l'objet d'un suivi prioritaire dans notre pays". *OCAM*. 28/07/2023. URL: ocam.belgium.be/700-extremistes-font-lobjet-dun-suivi-prioritaire-dans-notre-pays/
Europol a des programmes similaires au niveau européen, *cf.* URL: www.statewatch.org/news/2021/june/eu-growing-online-censorship-of-presumed-violent-extremism-of-all-ideological-varieties/
58 Audition du COC au Parlement Fédéral suite au rapport sur la BNG. 28/06/2023. *Op. Cit.*
59 Voir l'article 25 du RGPD. URL: eur-lex.europa.eu/eli/dir/2016/680/oj#art_25

En effet, les ANPR bruxelloises ont été annoncées simultanément comme une mesure antiterroriste et dans le cadre de la LEZ dans le but de lutter contre la pollution et d'améliorer la santé. Cependant, des autorisations ont rapidement été accordées pour leur utilisation dans le cadre du contrôle des zones piétonnes. Une taxe kilométrique a également été proposée, qui serait calculée sur base des trajets inférés des données collectées par les caméras.

Entremêlant l'analyse vidéo et les bases de données techniques, les caméras ANPR représentent un précédent décisif, particulièrement inquiétant si le même type d'association devait être étendu au domaine de la reconnaissance faciale – ce qui équivaudrait à un contrôle d'identité généralisé à tou·tes les passant·es.

2. Les risques liés aux bases de données policières : études de cas

Les bases de données policières comportent un grave risque de discrimination en raison des catégories utilisées, des informations qu'elles contiennent, et du manque de régulation concernant leur existence et leur contenu. Comme l'explique le criminologue Jan Van Dijk, les données policières « reflètent le problème de la criminalité tel qu'il est perçu par les forces de l'ordre et les hommes politiques, les procureurs ou les juges qui supervisent leur travail », dans la mesure où ces institutions sont « sujettes à leurs propres préjugés ».[60]

En vertu de la loi sur la fonction de police, la BNG, les banques de données de base et les banques de données particulières peuvent contenir des données à caractère personnel d'individus appartenant à des catégories spécifiques, et ce à des fins de police administrative comme judiciaire.[61]

À des fins administratives, il s'agit notamment des coordonnées des représentant·es d'associations, des personnes impliquées dans des incidents liés à l'ordre public, des membres d'un groupement national ou international susceptible de porter atteinte à l'ordre public, des personnes susceptibles de porter atteinte aux personnes ou aux biens mobiliers et immobiliers à protéger, et des personnes faisant l'objet d'une mesure administrative prise par une autorité administrative compétente et que les services de police sont chargés de suivre.[62]

La chercheuse en droit et avocate Catherine Forget souligne les conséquences néfastes pouvant découler de la conservation d'informations sur une personne dans une base de données policière :

> Cette problématique concerne toute personne dite « connue » des services de police dès lors que certaines informations la concernant sont enregistrées dans des banques de données, parfois même sans qu'elle n'en ait connaissance ou qu'elle

60 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. Cité dans Rémy Farge, 2023. "Police du futur et nouvelles technologies du profilage ethnique". *La chronique des droits humains*. pp. 13-16.

61 Article 44/5 de la loi sur la fonction de police du 5 août 1992. URL: ejustice.just.fgov.be/eli/loi/1992/08/05/1992000606/justel

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

> n'ait jamais fait l'objet de poursuites pénales. Cet enregistrement peut non seulement générer un sentiment d'incompréhension mais également provoquer des conséquences désagréables voire pénibles pour la personne visée. Celle-ci peut effet être contrainte de se soumettre à des contrôles d'identité renforcés à l'aéroport impliquant parfois un interrogatoire, subir des fouilles sans justification, ou encore, être dans l'impossibilité d'obtenir une attestation de sécurité dans le cadre de ses activités professionnelles la privant de facto de l'exercice de son métier.[63]

Les données contenues dans ces bases peuvent sembler anodines, mais elles peuvent avoir de graves conséquences. Dans son rapport d'activité 2022, le COC fait remarquer que :

> La qualité (l'exactitude et la précision) des banques de données policières laisse encore (trop) à désirer, ce qui a des retombées potentiellement très préjudiciables pour le citoyen. Celui-ci peut en effet être directement ou indirectement préjudicié par des traitements de données incorrects, dépassés ou autrement impropres. Directement, parce que le traitement dont le citoyen fait l'objet (fouille, arrestation, approche policière, lien avec les banques de données techniques ANPR, etc.) ne saurait être correct dès lors qu'il repose sur des informations erronées. Et indirectement, du fait qu'il est ainsi injustement fait obstacle ou mis un terme à l'accès à certains métiers : les (candidats) fonctionnaires de police, les agents de sécurité, les militaires, les travailleurs du secteur de la sécurité privée, les travailleurs d'une centrale nucléaire et autres sont tous jugés notamment sur leurs « antécédents policiers ».[64]

Plusieurs cas relevés par le Comité permanent de contrôle des services de police (Comité P), ont révélé que ces informations étaient utilisées sans précautions adéquates.[65] Par exemple, un cas concernait des informations selon lesquelles un individu était prétendument porteur du VIH et prévoyait d'infecter des policiers au cours d'une opération. L'enquête menée par le Comité P et le COC a permis de découvrir que les informations provenaient uniquement de rumeurs, sans aucun fondement juridique ou administratif pour leur enregistrement. Les informations reçues n'ont pas été évaluées de manière exhaustive et il n'y avait aucune raison tangible de les enregistrer dans la banque de données.[66]

A l'aune de ces constats, il est important de noter que, depuis l'adoption d'une réforme en 2019,[67] les services répressifs sont aussi autorisés à traiter des catégories particulières de données, y compris des données sensibles comme les données de santé, biométriques et génétiques, dans le cadre de leurs missions de police administrative et légale, ainsi que dans le contexte de la coopération policière internationale. Ces données biométriques sont, par exemple, les empreintes

63 *Ibid.*
64 COC. *Rapport d'activité 2022*. Organe de contrôle de l'information policière. URL: organedecontrole.be/files/Rapport-dActivit%C3%A9_COC_2022.pdf
65 Rosamunde van Brakel. 2021. "How to Watch the Watchers? Democratic Oversight of Algorithmic Police Surveillance in Belgium". *Surveillance & Society*, vol. 19, n° 2, pp. 228-240. URL: ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/14325/9779
66 Rapport d'activité 2003 du Comité permanent de contrôle des services de police. *Chambre des représentatns de Belgique et Sénat*. 30/07/2004. URL: comitep.be/document/jaarverslagen/2003.pdf
67 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

digitales, les traits du visage, la voix, l'empreinte des oreilles. Or, la collecte de ces informations nécessite un traitement minutieux en raison du risque de divulgation d'informations sensibles, telles que l'appartenance ethnique ou la santé d'une personne.[68]

Nous allons maintenant explorer plusieurs études de cas pour illustrer les risques spécifiques liés à l'utilisation des bases de données de la police. Nous examinerons tout d'abord des bases de données particulières, pour les travailleurs·euses du sexe d'une part et les "bandes" urbaines d'autre part. Ensuite, nous nous pencherons sur les politiques de lutte contre la radicalisation, ainsi que sur les *screenings* et les habilitations de sécurité. Enfin, nous conclurons cette section avec les récents litiges qui pourraient remettre en question l'approche actuelle en ce qui concerne le droit d'accès des individus à leurs données personnelles détenues par les services de police en Belgique.

a. Base de données et profilage de travailleurs·euses du sexe

Depuis 2022, le travail du sexe a été dépénalisé en Belgique.[69] Fournir des services sexuels n'a jamais été interdit en soi, mais il y avait auparavant un délit d'incitation et un délit de proxénétisme. En outre, il existait une forme de criminalisation indirecte, qui impliquait que toute personne gagnant de l'argent grâce au travail du sexe, même à plusieurs degrés de séparation, était considérée comme proxénète. Par conséquent, colocataire, chauffeur, comptable… pouvaient être condamné·es pour proxénétisme.[70]

Ce qui ressort toujours du domaine pénal, c'est la traite et le trafic d'êtres humains, ainsi que certaines formes de passation de marchés considérées comme abusives. Néanmoins, le fédéralisme belge laisse aux autorités locales une grande marge de manœuvre dans leur régulation du secteur et diverses mesures locales fixent souvent des restrictions à l'exercice du travail du sexe.

À Anvers, par exemple, le travail du sexe se concentre dans un quartier spécifique, le *Schipperskwartier*. Une équipe de police composée de 15 membres, connue sous le nom de *prostitutieteam*, est chargée de surveiller cette zone. La police procède à des inspections pour détecter des lieux de travail du sexe et engage des poursuites pénales pour les infractions les plus graves, telles que la traite des êtres humains. Toutefois, pour les infractions mineures telles que les nuisances sonores, les autorités locales interviennent en infligeant des sanctions administratives communales ou des fermetures en cas de perturbations de l'ordre public.

En 2020, la Ville d'Anvers a développé une plateforme appelée "HookUp" pour encadrer le travail du sexe de "vitrine". L'objectif déclaré de HookUp est d'empêcher la coercition des travailleuses·eurs du sexe et l'ingérence d'intermédiaires. HookUp

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

69 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

70 Entretien avec le coordinateur d'une association de soutien aux travailleurs·euses du sexe à Bruxelles, 04/08/2023.

est une plateforme destinée aux propriétaires ou gérant·es d'établissements, et aux travailleuses·eurs du sexe eux-mêmes. La création d'un profil sur la plateforme HookUp est obligatoire pour les personnes cherchant à louer un espace de travail dans le *Schipperskwartier*. Parallèlement, il est nécessaire de disposer d'un certificat d'aptitude et de licences spécifiques pour louer un établissement à des travailleuses·eurs du sexe. Pour obtenir les certificats et licences nécessaires, les candidats doivent fournir leurs informations personnelles, qui seront conservées jusqu'à cinq ans.

L'application recueille et transmet des données aux autorités locales, y compris des informations sur les lieux où les travailleuses·eurs du sexe exercent leur activité et sur la propriété des locaux. Le site web de la ville précise que les informations concernant les travailleuses·eurs du sexe ne sont accessibles qu'à la police, supposément dans le but de garantir leur sécurité.[71]

HookUp permet à la police d'avoir un aperçu des contrats de location conclus, de fournir une plateforme aux travailleuses·eurs du sexe pour signaler des comportements abusifs et partager des informations, telles que la photographie d'un violeur. De plus, la police utilise la plateforme pour confirmer l'identité des nouvelles travailleuses·eurs du sexe, collaborant avec la ville dans le but supposé de lutter contre la sous-location, la traite des êtres humains et d'autres activités définies comme criminelles.

Néanmoins, la police utilise également ces données pour d'autres objectifs. Il est évident qu'à première vue, garantir la sécurité des travailleuses·eurs du sexe et lutter contre la traite des êtres humains sont des objectifs légitimes. Cependant, lorsque cela se fait par le biais de la surveillance et du contrôle, les travailleuses·eurs du sexe sont exposées à un risque accru, en particulier pour celles qui sont les plus vulnérables.

La nature policière de la plateforme et l'obligation de s'inscrire dans la base de données ont pour conséquence pratique d'exclure les personnes en situation irrégulière ou précaire. L'anthropologue Anna Di Ronco, qui a mené des recherches sur le contrôle policier du travail du sexe à Anvers, écrit :

> Les travailleuses du sexe identifiées sont approchées par des policiers se faisant passer pour des clients et sont ensuite enregistrées dans la base de données policière lors d'une inspection administrative menée en tandem avec la ville. Au cours de ces inspections administratives, la police vérifie soigneusement la situation régulière des travailleuses du sexe migrantes (par exemple : "parfois, lorsqu'elles sont en situation irrégulière – nous sommes toujours la police et nous devons faire notre travail – il faut vérifier si elles peuvent rester en Belgique ou non").[72]

71 "Prostitutiebeleid". *Stad Antwerpen*. URL: www.antwerpen.be/prostitutiebeleid

72 Anna Di Ronco. 2022. "Law in action: Local-level prostitution policies and practices and their effects on sex workers". *European Journal of Criminology*. Vol. 19, n°5, pp. 1078-96. DOI: 10.1177/1477370820941406.

Comme le raconte Di Ronco, l'enregistrement obligatoire des travailleuses·eurs du sexe sur l'application HookUp pousse les travailleuses·eurs du sexe migrant·es d'Anvers vers des espaces moins visibles où elles sont moins susceptibles d'être soutenues par des associations :

> Les actions répressives de la police dans les rues ont également conduit les travailleuses du sexe, en particulier les travailleuses du sexe migrantes non européennes sans visa, à se déplacer à l'intérieur et à utiliser des sites Web et des applications en ligne, ce qui rend beaucoup plus difficile pour les travailleurs sociaux de les atteindre. En commentant la politique de gestion de la prostitution à Anvers, un travailleur social a suggéré : "cela a poussé certaines travailleuses du sexe à la marge, et même avec les meilleures intentions [...]. Essayer de trop contrôler pousse toujours les gens vers des espaces invisibles, comme les chambres, les appartements, Internet, où il est bien sûr plus difficile pour nous, en tant qu'organisation sociale, de les atteindre".[73]

Cette situation contraste fortement avec celle de Bruxelles, où la police des mœurs semble moins préoccupée par le statut migratoire des travailleuses·eurs du sexe. Le coordinateur d'une association locale de soutien aux travailleuses·eurs du sexe nous a décrit les relations entre les travailleuses·eurs du sexe et la police dans le quartier Yser, situé entre le centre de Bruxelles et la gare du Nord :

> Il y a une grande différence entre ce qu'ils appellent les "Playmobils" et les agents en civil. Les agents en civil font partie de la brigade des mœurs, tandis que les "Playmobils" sont des hommes ordinaires de la police locale de Bruxelles... Au sein de la brigade des mœurs, les flics entretiennent une relation très paternaliste avec les travailleuses du sexe d'Yser. Mais c'est du donnant-donnant, en d'autres termes, ils viennent et disent : « Comment allez-vous ? Y a-t-il des gens qui vous embêtent ? Est-ce qu'il y a des gens qui vous volent ? Y a-t-il de la drogue ? Y a-t-il des proxénètes dans le coin ? » Ils vont à la pêche aux informations. [...] On fait confiance à la police des mœurs, ils ne se préoccupent pas vraiment des sans-papiers. Ce n'est pas leur problème. Leur problème, c'est le racket, [...] c'est ce qui intéresse la brigade des mœurs, et c'est là qu'est leur intérêt, connaître les filles, savoir où elles travaillent et leur faire dire ce qui se passe. [...] Les flics locaux sont terribles parce qu'ils changent d'une semaine à l'autre. Une semaine, ils vous laissent tranquille, la semaine suivante, ils vous demandent : « Allez, bouge »... [...] Les flics de la ville sont donc très imprévisibles. [...] En fait, à Yser, tout ce que les filles demandent, c'est : « On se fiche que la police vienne nous voir, on veut juste savoir, on ne veut pas qu'on nous dise quelque chose de différent chaque semaine ».[74]

C'est pourquoi la dépénalisation du travail du sexe recueille un soutien quasi unanime sur le terrain, dans la mesure où elle améliore considérablement les conditions de vie des travailleuses·eurs du sexe et réduit les risques de contrôle pour les travailleuses·eurs migrant·es. Cependant, si la dépénalisation est largement soutenue, les avis sont moins tranchés en ce qui concerne la légalisation du travail du sexe. Par exemple, certaines associations font campagne depuis longtemps pour la reconnaissance d'un statut officiel pour les travailleurs du sexe, tandis que d'autres montrent moins d'enthousiasme à ce sujet. Un travailleur social local raconte :

73 *Ibid.*

74 Entretien avec le coordinateur d'une association de soutien aux travailleurs·euses du sexe à Bruxelles, 04/08/2023.

> 99,99 % des gens qu'on voit, ils n'en ont rien à foutre du statut de tds [travailleur·euse du sexe]. Ils n'ont pas de papiers, ils n'ont pas de maison, ils n'ont pas de mutuelle. Donc quand on leur dit : « tu vas pouvoir avoir un statut officiel TDS », ils disent « mais j'ai même pas de papelards, je m'en fous ». Donc moi, je suis content que les tds puissent avoir un statut si ce sont leurs revendications. Mais je porte pas ça, parce que je suis pas tds et ce ne sont pas les revendications des gens qu'on voit. Et donc du coup, tous ces enjeux de se déclarer ou pas comme TDS, c'est des trucs qu'on voit peu chez nous. Et du coup, je me dis, sachant qu'à Anvers, le profil des personnes est à peu près le même [...], j'imagine que l'appli en question [HookUp], si t'as pas de numéro national, pas de papier, je sais pas bien si tu vas t'inscrire dessus.[75]

Une nouvelle loi fédérale a été adoptée en 2024.[76] Elle autorise la collecte de grandes quantités d'informations pour réglementer le travail du sexe. Les plateformes en ligne, par exemple, doivent enregistrer l'activité sur leurs sites web et la fournir sur demande de la police. En outre, les potentiels employeurs doivent demander un permis, ce qui ouvre la voie à un registre des employeurs autorisés. Si veiller à ce que les personnes ayant un casier judiciaire pour des faits de violences sexuelles ne deviennent jamais employeuses est probablement louable, le travail du sexe pourrait recevoir son propre numéro de classification (code NACE), ce qui rendrait les travailleuses·eurs du sexe officiellement enregistrées et... traçables.[77] Il semble néanmoins qu'il soit possible (et légal) de s'enregistrer sous un autre code de manière à limiter les potentiels effets négatifs d'un tel enregistrement.[78]

L'introduction de ce nouveau cadre juridique nécessite une extrême prudence. A l'heure où certains au Parlement Fédéral envisagent l'extension du système HookUp à l'ensemble du territoire,[79] il est urgent d'imposer les principes de minimisation des données et de garantir la séparation des fichiers administratifs des fichiers de police, conformément au droit international — surtout si la sécurité de ces données ne peut être garantie.

En effet, en décembre 2022, la Ville d'Anvers a été victime d'une importante faille de cybersécurité lorsque des pirates informatiques se sont infiltrés dans ses systèmes. En conséquence, la Ville a dû temporairement revenir au papier et au crayon pour ses activités. Les pirates se sont emparés de plus de 500 gigaoctets de données, dont des données personnelles, des passeports, des cartes d'identité, des documents financiers, *etc*.[80] On ne sait pas si des données relatives au travail du sexe ont été divulguées, mais l'application HookUp a depuis cessé ses activités.[81] Les pirates ont émis une demande de rançon, avertissant que les données seraient divulguées si aucun paiement n'était effectué. Les pirates n'ont pas été

75 *Ibid.*
76 UTSOPI, 2024. *La loi belge du travail pour les travailleur·euses du sexe.* URL: www.utsopi.be/our-work/decriminalisation/cadre-du-travail
77 Entretien avec le coordinateur d'une association de soutien aux travailleuses·eurs du sexe à Bruxelles, 04/08/2023.
78 Selon une représentante d'UTSOPI qui a eu la gentillesse de nous fournir un retour sur cette section.
79 Question n°1070 du 25/02/2022 de Ben Segers, social-démocrate flamand, au ministre de la Justice. URL: www.lachambre.be/QRVA/pdf/55/55K0082.pdf
80 Michaël Temmerman. "Site van hackerscollectief Play dat stad Antwerpen viseerde, plots offline gehaald". *gva*. 21/12/2022. URL: www.gva.be/cnt/dmf20221221_95447283
81 Selon des échanges personnels avec un travailleur social local et avec le fonctionnaire en charge du travail du sexe à Anvers durant l'été et l'automne 2023.

arrêtés et les données n'ont pas été divulguées à grande échelle, ce qui laisse penser que la rançon a pu être payée, bien que le bourgmestre le nie.[82]

En 2022, la zone de police de Zwijndrecht, située dans la province d'Anvers, avait également fait l'objet d'une cyberattaque qui avait entraîné la fuite de « plaques d'immatriculation, de dossiers de police, de rapports d'enquête et d'amendes datant des 16 dernières années".[83] Ces incidents soulignent la vulnérabilité de ces infrastructures et mettent en garde contre les risques liés à la collecte centralisée de données.

b. Bases de données et profilage des "bandes urbaines" (BU)

Début des années 2010, une série d'actes violents et de décès imputés à des "bandes urbaines" a mené la police belge à faire de cet enjeu une priorité.[84] La création de bases de données afin de faciliter le suivi, la surveillance et le ciblage des membres présumés de ces supposées "bandes", a constitué un aspect central de cette démarche.

La qualification de "bande urbaine" conditionne la façon dont sont perçues les personnes comme les activités auxquelles elles prennent part. Elle renforce une lecture raciste des situations, propice à la prolifération de stéréotypes et de discours alarmistes. Les membres des "bandes" ont ainsi été comparés à des "enfants soldats" et des programmes "sociaux" ont été mis sur pied dans le but de leur faire comprendre que « la Belgique n'est pas l'Afrique » – alors même que la grande majorité de ces personnes sont nées en Belgique ou ont grandi dans le pays.[85]

Il est largement reconnu que les récits sur les "bandes urbaines" sont sous-tendus par des idéologies racistes et classistes, mobilisées pour cibler des jeunes issu·es de minorités.[86] Les individus identifiés comme faisant partie de ces "groupes problématiques" ont un profil commun : ils sont en position de vulnérabilité et sont victimes de discrimination.[87]

En effet, les paramètres définissant qui est inclus dans les bases de données sur les "bandes urbaines" sont extrêmement vagues. Comme l'explique Rémy Farge, de la *Ligue des droits humains* (LDH) :

> Du côté de la police, la définition beaucoup plus large englobe tout groupe de personnes perturbant l'ordre public et la sécurité. C'est cette dernière acception qui

82 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

83 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/

84 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

85 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/

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

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

sert d'outil d'investigation policière et de recueil d'information.[88]

La question a été posée au DPD de la zone de police de Charleroi, qui a lui-même reconnu que la collecte d'informations sur les membres de "bandes" est basée sur des corrélations plutôt que sur des faits, a-t-il déclaré :

> Il n'y a pas de définition formelle à proprement parler, il s'agit en fait de faits infractionnels qui sont constatés, régulièrement commis par les mêmes personnes ou sur le même territoire et qui créent un problème d'ordre public. Les corrélations ainsi établies (faits et personnes, relations entre personnes) sont proposées au magistrat de référence et la « bande » est ainsi créée. Il s'agit principalement d'une appellation vernaculaire.[89]

Ce flou entourant l'inclusion dans les bases de données sur les "bandes urbaines" présente des risques importants de discrimination fondée sur la classe et la "race".[90] Selon Rémy Farge, la collecte d'informations par la police sur les membres présumés de "bandes" sera largement influencée par les préjugés raciaux de chaque policier :

> L'analyse de la base de données de référence policière reprenant ces bandes urbaines indique que les chiffres, la localisation et le recensement de ces bandes « sont à relativiser, selon les représentations des policiers ».[91] Le recensement dépendrait aussi de l'agent verbalisateur : « Cette qualification dépend donc du hasard, de la perception du policier, du signalement par ce dernier ou de l'enregistrement dans la base de données » alors que « ces chiffres sont très souvent utilisés par les médias pour montrer une quelconque augmentation ou illustrer un fait divers. »
>
> Les statistiques policières ne constituent pas la réalité mais une image enregistrée de la délinquance ou de la criminalité et sont influencées par de multiples facteurs. Leur enregistrement dépend en partie des représentations des victimes et des institutions à l'égard du système pénal : « Dans ce système de représentations, certains individus ou groupes présentent une vulnérabilité particulière parce qu'en raison d'un ensemble idéologique complexe ils incarnent à un moment donné le sentiment d'une menace.[92] »[93]

Les conséquences d'un enregistrement en tant que membre d'une "bande" sont sérieuses. Le DPD de la zone de police de Charleroi écrit : « Le fait de pouvoir disposer de la photo permet au fonctionnaire de police, à l'occasion d'une patrouille de sécurisation, de pouvoir identifier le cas échéant la personne à surveiller, fouiller ou interpeller. »[94]

---

88 Rémy Farge, 2020. "Police du futur et nouvelles technologies du profilage ethnique". *La chronique des droits humains* n°191, pp. 13-16.

89 DPD de la zone de police de Charleroi dans ses réponses écrites à notre enquête. 02/03/2023.

90 Le concept de "race" est à comprendre ici au sens de construction sociale et non de catégoie biologique.

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

92 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*, n° 2, pp. 119-133.

93 Rémy Farge, 2023. "Police du futur et nouvelles technologies du profilage ethnique". *Op. Cit.*

94 DPD de la zone de police de Charleroi dans ses réponses écrites à notre enquête. 02/03/2023.

Les bases de données sur les “bandes urbaines” servent à faciliter les enquêtes, explique un policier, le langage déshumanisant utilisé étant révélateur du racisme en jeu :

> Par exemple, on arrache un sac à une vieille dame et elle nous dit que c’est une bande de trois ou quatre blacks. Elle sait donner la description de l’un des blacks. Donc on en a un. Qui sont les trois autres ? On ne le sait pas. On va vérifier dans l’ordinateur, on voit le dernier fait que ce type a fait et avec qui il l’a fait. Il a pu être arrêté des autres fois avec des autres. Et donc on va montrer des photos et comme ça, on avance petit à petit.[95]

Comme le souligne une récente étude sur le potentiel discriminatoire du programme i-Police (qui sera traité dans la troisième section), le système pénal belge a été épinglé à plusieurs reprises pour ses pratiques racistes, notamment en matière de profilage ethnique.[96] Le Comité des Nations Unies pour l’élimination de la discrimination raciale (CERD) a fait part en 2014 de ses préoccupations face aux « informations selon lesquelles les personnes d’origine étrangère sont surreprésentées dans le système de justice pénale, notamment du point de vue du taux et de la durée d’incarcération ».[97]

La branche belge d’Amnesty International a publié un rapport sur le profilage ethnique en 2018.[98] Ce rapport conclut que la moitié des policiers interrogés reconnaissent le problème du profilage ethnique. Si les agents comprennent la nécessité de disposer de motifs légitimes pour tous les contrôles, des consignes ambiguës ont conduit à une interprétation large de la loi et à une confiance accrue dans leur intuition. Amnesty note toutefois que cette intuition soit souvent associée à des stéréotypes, que les individus contribuent consciemment ou non à leur perpétuation.

Bien que la publication du rapport d’Amnesty International ait donné lieu à des débats publics au sein du Parlement fédéral,[99] la situation ne semble pas s’être améliorée, comme l’indique le rapport 2021 du CERD :

> Le Comité est préoccupé du fait que le profilage racial par la police continue d’être un problème persistant [...] et qu’il n’existe aucune loi interdisant explicitement le profilage racial. Le Comité est également préoccupé par l’existence d’un risque d’abus dans la pratique fondée sur l’interprétation du terme « motifs raisonnables » employé dans la loi [...] sur la fonction de police, en ce qui concerne les compétences des policiers pour effectuer un contrôle d’identité. Enfin, le Comité

95 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

96 Jérémiah Vervoort, 2021. *I-Police ou l’art de prédire la discrimination*. Travail de fin d’études. Bruxelles: Université libre de Bruxelles.

97 CERD. 2014. “Observations finales concernant les seizième à dix-neuvième rapports périodiques de la Belgique”. *Convention internationale sur l’élimination de toutes les formes de discrimination raciale*. cerd/c/bel/co/16-19. URL: tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CERD%2FC%2FBEL%2FCO%2F16-19

98 Amnesty International Belgique. 2018. ’On ne sait jamais avec des gens comme vous’. URL: www.amnesty.be/IMG/pdf/rapport_profilage_ethnique.pdf

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

> est préoccupé par le manque de données exhaustives, ventilées par appartenance ethnique ou origine nationale, sur les personnes visées par les contrôles d'identité et victimes du profilage racial ou ethnique.[100]

Une étude publiée en 2021 a confirmé cette situation problématique. Une enquête ethnographique menée dans deux zones de police belges a révélé que les contrôles d'identité étaient principalement influencés par ce que les policiers appellent leur "intuition", leur "sixième sens" ou leur "radar". L'intervention de la police à l'encontre des personnes est déterminée non seulement par leur comportement, mais aussi par leurs caractéristiques personnelles, notamment leur sexe, appartenance ethnique, âge, statut socioéconomique et habillement. De plus, « certains groupes sont associés à l'image de "fauteurs de troubles", ce qui, aux yeux des inspecteurs·trices en intervention, justifie une approche plus sévère ».[101]

Les préjugés de la police influencent son action, ce qui a pour conséquence de multiplier les interpellations, les arrestations et les privations de liberté de certains groupes. Dans ces conditions, il est difficile d'envisager comment la justice belge pourrait échapper à la critique de l'usage de données massives (*big data*) en matière policière comme terrain propice à la reproduction des discriminations.

c. Discrimination à l'embauche, *screenings* et habilitations de sécurité

En Belgique, les employés peuvent être sujets à des vérifications de sécurité (*screenings*) par leur employeur ou par une autorité publique. Ces contrôles ont lieu dans un certain nombre de circonstances, telles que pour des affectations ou des fonctions particulières, ou pour l'octroi de certains privilèges qui dépendent de l'examen de la loyauté, de l'intégrité, de la discrétion et de la "bonne moralité" générale de l'employé.

Ces *screenings* sont effectués sur base d'informations issues des bases de données policières, administratives et de sécurité. On peut citer les exemples suivants :

- une "habilitation de sécurité" avant de pouvoir prendre connaissance d'informations sensibles ;
- une "attestation de sécurité" avant de pouvoir exercer certaines fonctions lors d'événements diplomatiques (par exemple un sommet européen) ou d'accéder temporairement à des zones sensibles (par exemple au sein des infrastructures nucléaires) ;
- un avis de sécurité positif pour, ensuite, pouvoir obtenir un badge d'aéroport ou pouvoir présenter sa candidature à la Défense.[102]

100 CERD. 2021. "Observations finales concernant le rapport de la Belgique valant vingtième à vingt-deuxième rapports périodiques." cerd/c/bel/co/20-22. URL: tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CERD%2FC%2FBEL%2FCO%2F20-22

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

102 Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité. URL: beroepsorgaan.be

Les autorités peuvent accéder à un large éventail de sources pour l'octroi ou non de ces habilitations de sécurité : la base de données Schengen ; la base de données Interpol ; la BNG (voir *supra*) ; la banque de données policière opérationnelle particulière développée et gérée par la Direction centrale de la lutte contre la criminalité grave et organisée liées au terrorisme, au radicalisme et aux extrémismes ; les banques de données communes (voir *supra*) ; les bases de données judiciaires ; le "cadastre Limosa" (le registre des travailleurs·euses étrangères) ; les données et informations relatives aux personnes communiquées par la Direction générale Transport aérien à l'Autorité Nationale de Sécurité concernant la sûreté de l'aviation civile ; une base de données sur le travail illégal et la fraude sociale ; une base de données détenue par l'Agence Fédérale de Contrôle Nucléaire.[103]

Lors d'un entretien avec le COC, nous avons demandé quels types d'informations cela pouvait inclure :

> Tout. Des informations judiciaires, des informations solides mais aussi des informations "douces" (de police administrative ou judiciaire). Il peut s'agir de rapports indiquant que vous avez été suspecté de vol, mais que vous n'avez jamais été condamné, ou que vous avez accepté une transaction du ministère public, *etc.* Ces informations seront utilisées pour attribuer ou non une autorisation.[104]

Le site web de l'Organe de recours indique que dans le cadre d'une enquête de sécurité,

> [Les enquêteurs·trices] peuvent non seulement consulter les fichiers existants mais aussi effectuer une enquête complémentaire (enquête auprès du voisinage, de l'employeur…). Dans ce cadre, le conjoint et les autres personnes majeures qui cohabitent avec le demandeur peuvent également faire l'objet d'une enquête.[105]

En Belgique, ces vérifications approfondies sont obligatoires pour les personnes travaillant dans les ports, les aéroports ou les centrales nucléaires[106] mais deviennent progressivement plus courantes. Même les bénévoles lors de grands festivals, par exemple, sont soumis·es à des contrôles, comme nous le verrons plus loin. Il existe un certain nombre d'exemples de personnes dont l'accès à l'emploi a été refusé en raison des informations détenues à leur sujet dans les bases de données de la police.

Par exemple, en 2023, il a été annoncé que les travailleurs·euses du port d'Anvers seraient soumis à des procédures de contrôle dans le cadre de la lutte contre le trafic de stupéfiants. Bien que l'on ne sache pas encore quelles bases de données seront consultées dans le cadre de ces procédures, il est probable qu'il s'agira d'informations contenues dans les bases de données de la police. En février 2023, le site web officiel du Premier ministre indiquait :

103 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
104 Entretien avec Frank Schuermans (COC), 17/02/2023.
105 Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité. URL: beroepsorgaan.be
106 Entretien avec Frank Schuermans (COC), 17/02/2023.

> Le screening du personnel portuaire [a commencé]. Il concerne quelque 16 000 personnes occupant des fonctions sensibles au sein du port, qui seront contrôlées par les services de sécurité et de renseignement afin de détecter tout lien avec le crime organisé. Ce processus a commencé ces dernières semaines. Les différentes entreprises portuaires ont désigné des officiers de sécurité qui agiront en tant que personnes de contact. Ceux-ci font actuellement l'objet d'un screening approfondi de la part de la Sûreté d'État. Une fois eux-mêmes screenés, ils pourront transmettre les coordonnées du personnel qui doit faire l'objet d'un screening au sein de leur entreprise.[107]

De tels *screenings* représentent une menace importante pour l'égalité des chances, en particulier lorsque les contrôles deviennent obligatoires pour accéder à une gamme croissante de services et d'opportunités. L'accès des employeurs aux bases de données de la police, bien qu'indirect, recèle un sérieux potentiel de discrimination, comme l'illustre le témoignage suivant, dans lequel un jeune homme s'est vu refuser un emploi dans une association de jeunesse apparemment en raison d'informations le concernant contenues dans une base de données policière :

> Je suis un homme âgé de 22 ans. Il y a trois ans j'ai été victime d'une attaque à l'arme blanche. J'ai été poignardé de nulle part. Non seulement était-ce un coup dur physiquement, mais aussi mentalement.
>
> Pour me rétablir, l'aide à la jeunesse m'a beaucoup aidé. J'y vais depuis environ huit ans. Ces dernières années, j'ai été étroitement impliqué dans un projet dans lequel nous sommes déployés en tant que stewards lors d'événements qui ont lieu dans le quartier. J'adore faire ça et je reçois beaucoup de responsabilités. Parce que je me suis senti moi-même si peu en sécurité, je suis d'autant plus conscient du besoin que les gens ont de se sentir en sécurité. [...]
>
> Ça fait quatre ans que je fais du volontariat à titre de steward dans une maison de jeunes de la ville. Cet été, j'ai postulé une fonction à responsabilité. On m'a annoncé par courriel que j'étais embauché. Mais la veille de la signature de mon contrat, le coordinateur m'a dit que je ne pouvais pas commencer: je n'avais pas passé le screening avec succès. Il m'a référé à un agent de la police locale, qui a seulement pu me dire que le résultat du screening était négatif.
>
> Quand mon travailleur social de jeunesse est allé vérifier chez ses contacts à la police, ils lui ont fait savoir qu'aucun screening n'avait eu lieu. Le pire est qu'on m'a par contre bien permis de travailler comme steward dans le centre de jeunesse. J'ai accepté malgré tout parce que j'adore ce travail et que tous mes amis fréquentent le centre.
>
> Je n'en ai aucune preuve écrite. Je n'ai pas de casier judiciaire et je n'ai jamais eu d'ennuis avec la police.
>
> Sauf une fois, il y a longtemps, quand j'étais mineur. Je faisais des courses dans le quartier avec mon frère aîné. En même temps se déroulait une manifestation interdite d'une organisation islamiste extrémiste.

107 "Un commissaire national aux drogues et plus de police dans le Port d'Anvers pour lutter contre la mafia de la drogue". 16/02/2023. URL: www.premier.be/fr/un-commissaire-national-aux-drogues-et-plus-de-police-dans-le-port-d%E2%80%99anvers-pour-lutter-contre-la

> Nous nous sommes trouvés encerclés par la police. Mon frère a été autorisé de rentrer chez lui parce qu'il travaillait à l'époque en tant que journaliste, ce qui lui a permis de présenter une carte de presse. Moi, j'ai été emmené au poste de police. J'ai ensuite dû me rendre chez un fonctionnaire responsable des Sanctions Administratives Communales, qui m'a imposé un travail d'intérêt général.
>
> Je n'avais pas du tout l'intention de manifester. J'étais au mauvais endroit au mauvais moment. Le fonctionnaire m'avait assuré qu'il n'en resterait aucune trace dans mon casier judiciaire. Je pense cependant que je suis resté dans une base de données et que c'est la raison pour laquelle je ne passe pas les screenings. Même lorsque je veux prendre l'avion pour l'étranger, ils me sortent toujours de la queue pour un contrôle et me disent que je suis fiché.
>
> En septembre, j'ai l'intention de m'inscrire à la formation sur la sécurité. J'ai très peur de ne pas passer positivement par le screening là-bas non plus. Pourtant, c'est mon rêve de travailler dans le secteur de la sécurité.
>
> Je suis profondément affecté par cette situation. Je pense que la société est ingrate. J'ai déjà fait tant d'efforts pour les jeunes et l'aide à la jeunesse. J'ai déjà fait tellement de volontariat pour la ville. Ça fait mal d'être associé au terrorisme.[108]

Ce témoignage met en lumière les conséquences des préjugés racistes et islamophobes dans la police, qui se reflètent ensuite dans les bases de données policières. Le jeune homme a manifestement été indûment enregistré dans une base de données l'associant au terrorisme en raison de la couleur de sa peau et de sa (supposée) religion. Son expérience révèle également la persistance de ces données dans des fichiers de police. Des années après les faits, les informations à son sujet mènent toujours à des interrogatoires et à des fouilles dans les aéroports et affectent encore ses chances de décrocher un emploi.

Cette histoire met en évidence les graves préjudices que les bases de données policières peuvent causer en renforçant les discriminations et injustices existantes.

D. *Screenings* antiterroristes

Outre le *screening* effectué pour les habilitations de sécurité, la police procède également à certaines analyses préventives et automatisées. Bien qu'il y ait peu d'informations disponibles à ce sujet, le porte-parole de la Police Fédérale a déclaré en 2018 :

> Au demeurant, nos services de police et de renseignement utilisent déjà des logiciels comme Radix et Vera 2 afin d'estimer les risques et les menaces dans la lutte contre le terrorisme. Divers paramètres et noms de suspects sont ainsi confrontés entre eux en vue de déterminer les priorités. Nos services utilisent les mêmes paramètres que ceux d'autres pays, mais en les adaptant au contexte national et en donnant des noms différents aux outils, comme Kim aux Pays-Bas et RADAR-iTE en Allemagne.[109]

108 Cité dans Nina Henkens et Ikrame Kastit. *La politique de déradicalisation vue sous un autre angle*. Uit de Marge. 2019. URL: www.uitdemarge.be/?sdm_process_download=1&download_id=5751

109 Lars Bové. "Politie gaat criminaliteit via data voorspellen". *De Tijd*. 30/08/2018. URL: www.tijd.be/politiek-economie/belgie/federaal/politie-gaat-criminaliteit-via-data-voorspellen/10044356.html

Ces questions ont été mises en évidence à la suite des attentats de Paris en novembre 2015 et des attentats de Bruxelles en mars 2016. Des mesures de lutte contre la radicalisation ont été mises en œuvre en Belgique dans l'objectif de préserver la sécurité nationale, et ont eu des répercussions importantes sur les personnes. Nadia Fadil, professeure de sociologie (KU Leuven), a coordonné une recherche sur les effets des procédures antiterroristes sur les musulmans en Belgique. Ces procédures ont pour conséquence des évaluations de sécurité négatives, des obstacles à l'accès aux services financiers, des refus aux frontières, des descentes de police répétées et des contrôles excessifs.

Les contrôles excessifs et constants constituent une forme de surveillance, voire de harcèlement, qui perturbent la vie personnelle des individus visés et portent atteinte à leur liberté. Ces pratiques violent non seulement les libertés individuelles et la vie privée, mais créent également un climat de peur et de méfiance.[110]

Dans de nombreux cas, le premier élément déclencheur des soupçons de la police est le fait qu'une personne a des connaissances, des ami·es ou des membres de sa famille partis en Syrie et soupçonné·es d'avoir rejoint Daesh (aussi connu sous le nom d'État islamique). Cette approche de la culpabilité par association a injustement piégé des personnes qui n'étaient pas elles-mêmes impliquées dans des activités illégales.

La participation à des associations, en particulier celles qui défendent la justice sociale ou des points de vue critiques, a servi de base pour cibler des individus. Cela revient à confondre dissidence et extrémisme, ce qui porte atteinte au droit fondamental à la liberté d'association.[111] Par ailleurs, le Comité de vigilance en matière de lutte contre le terrorisme (Comité T) a consulté des cabinets d'avocat·es s'occupant de contestations de refus d'habilitations, ceux-ci soulignent « la surreprésentation de Belgo-Marocain·nes ou de personnes d'origine maghrébine se trouvant dans cette situation, en particulier dans les cas de non accréditation dans le secteur aéroportuaire ».[112]

Les effets de ces politiques préjudiciables sont importants et variés. Des personnes ont subi des pertes financières et ont eu des difficultés à trouver un emploi en raison de leur exclusion du système bancaire. Ces difficultés financières exacerbent leur vulnérabilité et peuvent paradoxalement les inciter à se radicaliser.[113]

Cependant, un autre rapport de l'équipe de Nadia Fadil indique que le concept de radicalisation lui-même doit être questionné. Les professionnels de la prévention font preuve d'un grand scepticisme à l'égard du terme et de son application, et plaident pour sa remise en question :

110 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.
111 *Ibid.*
112 Comité T. Rapport 2021. *Op. Cit*. p. 41.
113 Nadia Fadil *et al*. 2022. "Entre droits fondamentaux et surveillance." *Op. Cit*.

> Les acteurs interrogés sont pour la plupart critiques à l'égard du thème de la radicalisation. Ils affirment que ce discours contribue à la stigmatisation des jeunes et remettent en question l'idée que la radicalisation est un danger ou un problème. Quelques-uns défendent le droit des jeunes à se retourner contre la société, à revendiquer leurs droits ou à soulever des problèmes, sans y voir immédiatement un danger. Les praticiens s'interrogent également sur la détection précoce de la radicalisation. Ils ont des doutes quant à l'opportunité et à la possibilité d'une telle détection : non seulement cela peut miner la relation de confiance, mais ils suggèrent également que le profil est vague et basé sur des stéréotypes ou des caricatures. En outre, l'évaluation est considérée comme une tâche difficile, voire impossible.[114]

Ces problèmes risquent fort de devenir plus fréquents à l'avenir avec la mise en œuvre prochaine de ce que l'on appelle « l'approche administrative communale ». Soutenu par la ministre de l'Intérieur, ce plan implique que les autorités locales prennent en considération les dossiers de police lorsqu'elles décideront de rejeter, de suspendre ou de retirer les licences des établissements et des entreprises locales ou de les fermer.[115]

D'autre part, l'efficacité d'une telle surveillance généralisée est discutable. Les services de sécurité contrôlent depuis des années les données des personnes voyageant par avion et ont traité des dizaines de millions de dossiers de passagers. Un rapport du coc pointe de nombreux problèmes et se demande si cette « ingérence profonde dans la vie privée » est efficace dans la lutte contre le terrorisme et la criminalité organisée.[116] De plus, ceci est illégal au regard de la jurisprudence de la Cour de Justice de l'UE et de la Cour constitutionnelle belge.[117]

Enfin, ces contrôles, conçus pour garantir la sécurité, s'appuient sur une pléthore d'informations disponibles. Toutefois, la qualité de ces sources d'information suscite des inquiétudes. Certains dossiers sont générés à des fins de renseignement et peuvent contenir des conjectures et des déductions infondées. Le problème essentiel réside dans l'origine de ces sources peu fiables, qui proviennent des forces de l'ordre ou des services de renseignement. Cela crée une situation problématique, car les individus n'ont pas d'accès direct à ces sources, ce qui les empêche de contester les informations éventuellement erronées.

---

114 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.

115 Loi du 15 janvier 2024 relative 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'Evaluation de l'Intégrité pour les Pouvoirs publics . URL: www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&pub_date=24-02-07&numac=2024000706
Institut fédéral pour la protection et la promotion des droits humains (IFDH). Avis n° 13/2022 du 28 octobre 2022. URL : web.archive.org/web/20230521154146/https://www.institutfederaldroitshumains.be/sites/default/files/2022-11/Avis%20IFDH%20Approche%20administrative%20communale_0.pdf

116 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

117 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. Vers un droit d'accès *direct* ?

Le droit d'accès aux données policières est inscrit à l'article 14 de la "Directive Police-Justice" (2016/680) de l'UE – le pendant du RGPD pour les forces de l'ordre.[118] Cet article stipule qu'une personne devrait avoir le droit « d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données », ainsi qu'une série d'informations sur ces données. Ce droit d'accès permet aux citoyen·nes d'exercer leur droit notamment à l'effacement et à la rectification.[119]

En principe, ce droit d'accès doit pouvoir être exercé de façon directe. Cependant, l'État belge ne prévoit qu'un accès indirect aux données traitées à des fins policières, contrairement à la plupart des États européens. Cela signifie que les demandes d'accès sont introduites auprès du coc et non du responsable de traitement des données. L'article 42 de la loi belge relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel stipule que le COC « communique uniquement à la personne concernée qu'il a été procédé aux vérifications nécessaires ».[120] Il est impossible de consulter les données elles-mêmes. Cette limitation de l'accès est si sévère qu'elle peut difficilement être considérée comme compatible avec le droit d'accès prévu par le cadre législatif européen.

Cette situation problématique a été portée devant la Cour de justice de l'Union européenne (CJUE). L'affaire a été introduite par une personne qui s'est vu refuser un emploi dans un festival en raison de son incapacité à obtenir une attestation de sécurité. L'avocate Catherine Forget, en partenariat avec la *Ligue des droits humains* (LDH), a obtenu une victoire historique devant la CJUE. Il s'est avéré que le refus d'attestation résultait d'informations concernant la participation du demandeur à dix manifestations dans le passé (sans avoir fait l'objet d'interpellations ni de poursuites d'aucune sorte).

Le demandeur a exercé son droit d'accès auprès du COC, qui a répondu que « toutes les vérifications avaient été effectuées ». En conséquence, le demandeur n'a pas pu prendre connaissance des accusations portées contre lui, et encore moins s'y opposer. En outre, la raison pour laquelle l'exercice d'un droit fondamental – le droit de manifester – a été enregistré dans une base de données de la police n'est pas claire.

La CJUE a jugé que la limitation du droit d'accès à un seul accès *indirect* aux bases de données policières est contraire à la loi européenne.[121] L'exercice indirect de ce droit avait à l'origine été conçu comme une garantie supplémentaire, à laquelle recourir lorsque des limitations s'appliquent, mais ne devrait pas être la seule voie disponible. Par conséquent, l'État belge devra revoir son cadre législatif pour remédier à cette situation.

118 "Directive police justice". *EUR-Lex*. 27/04/2016. URL: eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016L0680

119 Art. 16 de la directive 2016/680. URL: eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680

120 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

121 CJUE. Affaire C333/22. Arrêt de la Cour (Cinquième chambre). *Curia. 16/11/2023.* URL: curia.europa.eu/juris/document/document.jsf?text=&docid=279747&cid=12850052

3. L'avenir des bases de données policières en Belgique

Suite à la publication par le COC d'un rapport très critique sur la gestion des bases de données policières,[122] son directeur, Frank Schuermans, a été invité au Parlement fédéral pour débattre de la question, où il a présenté les conclusions suivantes :

- les systèmes informatiques de la police datent de l'époque "préhistorique" et leur entretien nécessite un travail considérable ;

- il y a un manque de standardisation, un manque de lignes directrices claires. Les différences dans la gestion de l'information entre les forces de police sont donc très importantes. Certains départements et zones de police y attachent une grande importance alors que d'autres aucune ;

- la formation dans les académies de police est insuffisante. Il n'y a pas de curriculum, pas de syllabus sur la protection des données. Les nouvelles recrues sont donc mal formées sur ces questions ;

- les responsables manquent d'expertise. Il y a encore des zones de police où il n'y a pas de DPD ou où le DPD a deux casquettes : DPD et directeur des opérations ou it manager en même temps, ce qui crée un conflit d'intérêt.[123]

Comme le montrent les différents cas présentés au cours de cette section, les individus et groupes racisés ou marginalisés sont particulièrement exposés à différentes mesures prises par les autorités en raison des informations présentes dans les bases de données policières. Le problème est particulièrement aigu dans le contexte de la surveillance des "bandes" urbaines, et dans le cadre des procédures de lutte contre le terrorisme. À la suite du rapport d'Amnesty International de 2018 sur les pratiques racistes de la police,[124] des discussions ont eu lieu au sein du Parlement fédéral concernant les méthodes de maintien de l'ordre qui recourent au profilage ethnique.[125] Toutefois, à l'heure actuelle, il n'y a visiblement aucune volonté politique de relever les défis de la gestion des bases de données et les conséquences discriminatoires qui en découlent pour les personnes les plus marginalisées.

122 COC, 2023. DIO23001. *Op. Cit.*
123 Audition du COC au Parlement Fédéral suite au rapport sur la BNG. 28/06/2023. *Op. Cit.*
124 Amnesty International. 2018. *Belgique : Le profilage ethnique, injuste et inefficace*. URL: www.amnesty.be/infos/actualites/article/belgique-profilage-ethnique-injuste-inefficace
125 Nawal Ben Hamou. 2019. "Le profilage ethnique". *Chambre des représentants de Belgique.* 54K3683001. URL: www.lachambre.be/FLWB/PDF/54/3683/54K3683001.pdf

III. Le projet fédéral “i-Police”

Le projet i-Police et ses ramifications sont au cœur de ce rapport sur la police “prédictive”. Il s’agit d’un plan fédéral doté d’un financement important, qui risque d’avoir de sérieux impacts sur les droits humains et les libertés fondamentales.

Dans un communiqué du ministère de l’Intérieur de 2022, le commissaire général de la Police Fédérale promettait que

> i-Police fera de la police belge l’une des forces de police les plus avancées d’Europe en termes de gouvernance des données. Le système analysera les informations, les mettra automatiquement à la disposition des forces de police, fera des propositions d’enquête et fournira de nombreux outils pour gagner du temps, comme les traductions automatiques. i-Police nous permet de frayer le chemin pour une Police Intégrée orientée vers l’avenir, au service des citoyens.[126]

Le même communiqué indique que

> 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.[127]

La première mention du projet i-Police que nous avons pu trouver remonte à la note de politique générale de 2013 de la ministre de l’Intérieur. La note indiquait que le projet i-Police visait à harmoniser les systèmes informatiques de la Police Fédérale (FEEDIS) et de la police locale (ISLP).[128] Les deux applications informatiques étaient – et sont toujours – obsolètes et coûteuses à maintenir : ISLP a été développé au début des années 90 et feedis au début des années 2000.[129]

En 2014, une étude de faisabilité relative à i-Police a été réalisée, et à cette occasion, la description du projet a été élargie. La note d’orientation de 2015 du ministre de l’Intérieur affirme que

> [i-Police] vise, à travers des réseaux de capteurs, à intégrer les informations collectées de manière intelligente aux niveaux local et fédéral avec les sources (authentiques) fermées et ouvertes actuelles afin d’exploiter ensuite au maximum ces informations en les traitant à l’aide d’outils intelligents automatisés. Équiper la police de technologie *“next generation”* au sein de la chaîne policière permet de pratiquer

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

127 *Ibid.*

128 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

129 GPI. 2020. Annexe H de la description du marché i-Police.

> un *intelligent policing*, c'est-à-dire une fusion de fonctions de police orientée vers la communauté, axée sur la résolution de problèmes et guidée par l'information..[130]

En 2016, le gouvernement fédéral belge a alloué des fonds pour la mise en place de i-Police, visant à centraliser toutes les données de la police au sein d'un même *cloud*. Le lancement opérationnel du système, alors prévu pour 2020, était le fait d'une collaboration entre le ministère de l'Intérieur, l'Agenda numérique et le ministère de la Justice.[131] On peut lire dans le plan de sécurité nationale 2016-2019 :

> Dans le domaine de l'*intelligent policing*, la Police Fédérale œuvre à une nouvelle solution innovante (*"i-police"*) consistant à renoncer au mainframe actuel au profit de technologies nouvelles et modernes. Celles-ci doivent permettre de mieux "relier", échanger et analyser les informations, et ce rapidement. La police doit en effet pouvoir travailler et agir sur la base d'une analyse intégrale d'informations structurées et non structurées, disponibles aux niveaux interne et externe.[132]

En septembre 2018, la Police Fédérale et les polices locales ont publié un communiqué de presse conjoint décrivant les projets de police "prédictive" dans le cadre de i-Police.[133] Ils envisageaient le lancement d'expériences de police "prédictive" à Anvers et dans d'autres zones de police au cours de la législature suivante, après les élections municipales du 14 octobre 2018. Les données d'analyse proviendraient des bases de données policières et engloberaient des facteurs tels que la fréquence de certains délits dans des zones spécifiques. Les sources de données externes étaient perçues comme tout aussi importantes.[134]

Figure 8. Le logo i-Police[135]
Source: *Rapport annuel 2022 de la Police Fédérale*, p. 82.

130 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

131 Rosamunde Van Brakel. *Automating Society 2019: Belgium*. *Op. Cit.*

132 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

133 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/

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

135 Selon un haut gradé de la police judiciaire fédérale, la ligne orange centrale symbolise la collecte des données, la ligne bleu clair la création de valeur à partir de ces données, tandis que l'ensemble du processus est protégé par l'épais bouclier bleu foncé.

En 2021, la Police Fédérale a lancé un appel d'offres pour un marché public,[136] attribué à la société française d'informatique et de conseil Sopra Steria pour 300 millions d'euros.[137] Le budget est réparti sur sept ans, de 2021 à 2027. La réalisation du projet devrait durer quatre ans, avec trois années supplémentaires de maintenance.[138]

L'appel d'offres comprend une fiction décrivant une journée dans la vie de "Jean", policier dans une zone de police imaginaire. L'intention de faire de i-Police un programme de police "prédictive" y est clairement exprimée. On peut y lire, par exemple :

> Un "pop-up" apparait [...] afin de signaler qu'une "anomalie", donc quelque chose d'inhabituel, a été constatée. L'application policière a enregistré un nombre élevé de vols de bicyclettes autour d'un certain endroit et à certains moments. Le système peut détecter cela parce que nos "data scientists" à Bruxelles ont programmé le système pour reconnaître des "anomalies" de ce type. [...] Le système indique que certains agissements suspects ont été récemment signalés à cet endroit. [La commissaire] prévoit une patrouille récurrente.[139]

Ou ailleurs, à propos du plan de prévention d'une zone de police :

> Grâce à l'analyse informatisée d'un certain nombre d'incidents récents et des accidents de la circulation, et l'ouverture prochaine d'une nouvelle Zone PME [petites et moyennes entreprises], un modèle « prédictif » sera réalisé et un plan pour la surveillance préventive des bâtiments des PME sera mis au point.[140]

Plus loin, un autre type d'application "prédictive" y est envisagé :

> Le service intervention et la direction des opérations organisent avec quelques zones voisines une action dans le but d'exécuter un contrôle de grande envergure dans les cafés et discothèques parce qu'une augmentation de la criminalité à l'aide d'armes blanches a récemment été constatée le vendredi soir.[141]

Le système est également imaginé pour permettre une surveillance accrue des personnes jugées suspectes :

> Jean reçoit encore en fin de journée un appel d'un enquêteur de Bruxelles. Du texte dicté lors du contrôle d'un lieu de résidence, il apparait qu'une autre personne était présente dans cette maison. Cette personne est suivie dans le cadre d'une enquête terrorisme. Le collègue de Bruxelles – qui avait pris un « abonnement numérique » sur la personne que Jean avait rencontré – voudrait obtenir de Jean des informations supplémentaires compte tenu qu'il a reçu une « alerte » automatique lui signalant qu'un agent de quartier d'une zone quelque part dans le pays (Jean en l'occurrence), a fortuitement rencontré cette personne dans le cadre de ses contrôles.[142]

136 "Marché i-Police". *Tenders electronic daily*. 2021. URL: ted.europa.eu/udl?uri=TED:NOTICE:675394-2021:TEXT:FR:HTML&src=0&tabId=4
137 Sopra Steria company. URL: www.soprasteria.be
138 Réponse de la ministre Verlinden à la question 1323 d'Yngvild Ingels, députée nationaliste flamande au Parlement Fédéral. 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
139 Annexe H de la description du marché i-Police, p. 35
140 *Ibid.*
141 *Ibid.*
142 *Ibid.*

1. Le "lac de données" i-Police

Les données contenues dans les bases de données de la police belge, ainsi que de nombreuses autres sources de données, alimenteront le futur programme i-Police. Comme l'illustre la courte fiction issue de l'appel d'offres i-Police, à la suite d'un contrôle d'identité :

> Leur système vérifie automatiquement dans 10 banques de données de contrôle (registre national, bases de données policières nationales et internationales, détention, *foreign fighters*…) et présente en temps réel les identités pour lesquelles il y a un *hit*. Seules les personnes devant faire l'objet d'un contrôle approfondi devront attendre à l'écart.[143]

La police prévoit d'inclure énormément de sources de données dans i-Police, comme le montre la figure ci-dessous.

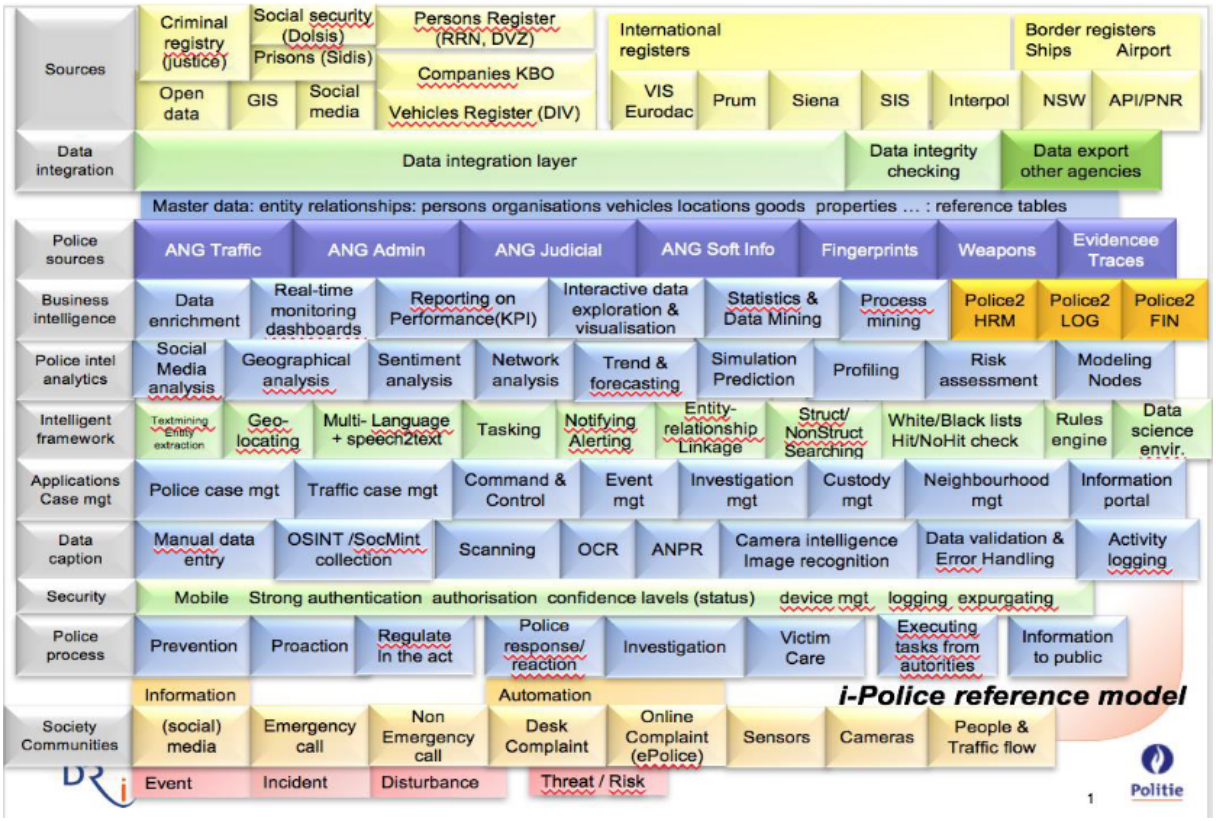

Figure 9. Architecture commerciale à venir du futur projet i-Police
Source : Annexe H de la description du marché i-Police. p. 58.

Au delà de leur quantité, c'est aussi la forme dans laquelle seront les données qui est source d'inquiétude. Les données provenant de diverses bases de données seront rassemblées dans un "lac de données" (*data lake*), c'est-à-dire un référentiel qui permet de rassembler de nombreuses données issues de différentes sources, tout en les conservant dans leur format d'origine. Les bases de données de la police font généralement la distinction entre les informations "validées" et "non validées". Les informations "validées" ont été vérifiées, tandis que les informations "non validées" ne l'ont pas été. Le COC s'inquiète de la combinaison d'informations vérifiées et non vérifiées dans le "lac de données" de i-Police :

143 *Ibid.*, p. 36

> Il y a beaucoup d'informations non validées. [...] Je crains que la différence entre informations validées et non validées soit noyée dans le lac de données de i-Police. Le policier moyen [...] aura donc accès à beaucoup plus d'informations et à beaucoup plus d'informations non validées, ce qui est bien sûr très inquiétant, et pas seulement pour la personne elle-même (présumée suspecte), mais aussi pour le système judiciaire dans son ensemble. C'est une grande source d'inquiétude pour tout le monde. [...] Mais c'est clairement la voie que la police, mais aussi la politique et les ministres [...] veulent suivre : donner à chaque officier de police autant d'informations que possible. [...] Dans notre système, il est tout à fait possible [...] que vous ayez été acquitté par le tribunal, mais que vous figuriez toujours dans une base de données et que, lorsque vous rencontrez un officier de police, il vous confronte aux données sur la base desquelles vous avez été acquitté par le tribunal. Il s'agit là d'un problème majeur.[144]

Compte tenu de sa longue expérience en tant que criminologue et ancien membre du Comité P, nous avons demandé au directeur du COC son avis sur l'évolution de la gestion de l'information au sein de la police :

> On a fait un très grand pas en avant avec la mise en place de la police intégrée, car avant ça, on avait la gendarmerie, la police communale et la police judiciaire. Mais en réalité, l'intégration n'a jamais été complète. Je parle souvent de « police désintégrée », car en réalité, même la gestion de l'information policière, qui devrait être un domaine où c'est intégré, on n'y est toujours pas. Heureusement, la BNG est centralisée, mais même à ce niveau-là, il y a de grosses différences dans les manières de travailler, d'encoder les données : le niveau de compétence est très faible. Donc si vous me demandez mon avis quant à l'évolution de la gestion de l'information, je dois dire que je suis relativement pessimiste. Les services qui devraient être intégrateurs de l'information policière sont les CIA (carrefours d'information d'arrondissement)[145]. En pratique, quand on veut se débarrasser d'un policier, c'est là qu'on le met. Ça en dit long, non ?[146]

Le "lac de données" de i-Police semble donner la priorité à la quantité plutôt qu'à la qualité. Cette approche est préoccupante car elle ne tient pas compte de l'exactitude et de la fiabilité des données alors que les implications soient loin d'être insignifiantes. Dans cette croisade pour amasser autant de données que possible au mépris du principe de minimisation, la devise de i-Police pourrait bien être : « Prenez-les tous ; l'algorithme reconnaitra les siens ».

2. Vidéosurveillance

Parmi les nombreuses sources d'information envisagées, le projet i-Police prévoit d'intégrer les images de vidéosurveillance. Cette section couvre les différents types d'analyse d'images utilisés par les forces de police, et notamment la reconnaissance faciale, déjà utilisée par la police belge.

Une première catégorie de logiciels est dédiée à la détection d'événements en

144 Entretien avec Frank Schuermans (COC), 17/02/2023.
145 "Les carrefours d'information d'arrondissement (CIA) constituent le lien entre les niveaux fédéral et local sur le plan de l'échange opérationnel d'informations de police administrative et judiciaire". URL: www.police.be/5998/fr/a-propos/police-integree/presentation
146 Deuxième entretien avec Frank Schuermans (COC), 11/10/2023.

direct. La police les utilise pour recevoir des alertes lorsque des activités jugées suspectes sont repérées, telles qu'un dégagement de fumée, un graffiti, un dépôt clandestin, une personne qui court ou qui traine à proximité d'une voiture, *etc*. En pratique, il est extrêmement fréquent que des séquences soient identifiées comme problématiques, avec un taux élevé de faux positifs, c'est-à-dire d'alertes injustifiées, amenant souvent les opérateurs·rices à les négliger. Il reste que ces technologies peuvent nuire à la vie privée et amener des perceptions biaisées des événements, dans la mesure où es critères et priorités de ces logiciels sont façonnées par les capacités techniques des logiciels ou par les représentations des informaticien·nes plutôt que par le débat démocratique.[147]

Dans le cadre d'enquêtes, la police belge utilise aussi le logiciel israélien BriefCam[148] pour analyser rétrospectivement des images.[149] Ce logiciel génère des résumés vidéo en condensant des heures de séquences filmées, pour ensuite classer les incidents en fonction de critères tels que les effets personnels des suspects, la couleur de leurs vêtements, ou leur genre. Ce dernier critère est questionnable, dans la mesure où la loi belge sur la non-discrimination permet des recherches ciblées basées sur des critères objectifs, qui peuvent inclure des caractéristiques physiques jugées sensibles. En revanche, le tri massif d'individus sur la base de tels critères est interdit.

BriefCam est utilisé tant par les zones de police locales que par la police judiciaire fédérale, mais ce logiciel a la particularité d'intégrer la possibilité d'effectuer de la reconnaissance faciale. Les zones de police locales ont tendance à nier l'utilisation de cette fonctionnalité.[150] La Police Fédérale, quant à elle, ne cache pas son usage : cette fonctionnalité fait d'ailleurs partie de l'appel d'offres qu'elle a récemment publié pour le renouvellement de ses licences BriefCam.[151] Il n'existe pourtant pas de cadre légal spécifique pour ce faire en Belgique.[152]

La reconnaissance faciale a plusieurs fois attiré l'attention de la presse belge ces dernières années. En 2017, la Police Fédérale avait lancé un projet pilote à l'aéroport de Zaventem pour la tester sur les voyageurs·ses.[153] Cependant, le système produisait un nombre important de faux positifs lors des tests, ce qui avait conduit à sa suspension. Malgré cela, une visite ultérieure du COC avait révélé que le système restait partiellement opérationnel, en dehors de tout cadre légal. À la suite

147 Sarah Brayne. 2020. *Predict and Surveil: Data, Discretion, and the Future of Policing*. New York: Oxford University Press.
148 BriefCam company. URL: www.briefcam.com
149 Nicolas Bocquet. 2021. "La Smart City à Bruxelles : quand « intelligence » rime avec vidéosurveillance". *Brussels Studies*. URL: journals.openedition.org/brussels/5655
150 "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
Nous avons également interrogé une zone de police qui utilise BriefCam à Bruxelles, celle-ci nous a fourni une réponse similaire.
151 Cahier spécial des charges n° 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
152 L'accord de gouvernement "Arizona" prévoit cependant de légaliser la reconnaissance faciale, *cf. Déclaration gouvernementale*, 04/02/2025, p. 145. URL: www.lachambre.be/flwb/pdf/56/0020/56K0020001.pdf
153 Rosamunde van Brakel. 2021. "How to Watch the Watchers? Democratic Oversight of Algorithmic Police Surveillance in Belgium". *Surveillance & Society*, vol. 19, n° 2, pp. 228-240. URL: ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/14325/9779

de l'enquête de l'Organe de contrôle, le projet avait finalement été abandonné.[154]

Par la suite, c'est l'utilisation du système de reconnaissance faciale Clearview AI qui avait alarmé la presse. Clearview est réputé pour collecter massivement des photos à partir de sources accessibles au public, telles que les réseaux sociaux. En août 2021, un site d'information a rapporté que la Police Fédérale avait effectué des recherches à l'aide de l'application Clearview.[155] La police a d'abord nié l'avoir utilisé, mais le coc a mené une enquête qui a fini par donner raison à la presse, malgré les dénégations répétées de la ministre de l'Intérieur devant la Chambre des représentants.[156] Il a ensuite été révélé que la licence pilote avait été fournie par Clearview lors d'un événement coordonné par Europol.

Ces développements en matière de vidéosurveillance suscitent de sérieuses préoccupations. Ils montrent que les usages policiers manquent cruellement de transparence, ce qui permet à la police d'agir en dehors du cadre légal et même de mentir aux autorités de contrôle lorsqu'elle est prise la main dans le sac.

Au vu des exemples d'usage de la vidéosurveillance par la police belge, la perspective d'une i-Police intégrant des logiciels d'analyse de comportement, de reconnaissance de plaques minéralogiques et de reconnaissance faciale dessine un panoptique des plus dystopiques. Il est indispensable de mettre un terme à cette expansion débridée de la vidéosurveillance. La *Ligue des droits humains* (LDH), ainsi que plusieurs autres associations, partagent cette position et mènent une campagne pour l'interdiction de la reconnaissance faciale dans l'espace public, sous le hashtag #ProtectMyFace.

Figure 10. La campagne #ProtectMyFace
Signez la pétition visant à interdire l'utilisation de la technologie de reconnaissance faciale dans les espaces publics à Bruxelles.

154 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

155 Ryan Mac, Caroline Haskins & 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

156 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. Recherche en sources ouvertes (OSINT), analyse algorithmique et sous-traitants

Outre ses propres bases de données et images de vidéosurveillance, la police souhaite intégrer des sources externes dans i-Police. Ce souhait a été exprimé à plusieurs reprises par les polices locales, la Police Fédérale et les criminologues engagés dans l'avancement de la police "prédictive". Par exemple, l'appel d'offres i-Police cite comme sources potentielles :

- les données des tierces parties sont les données saisies et gérées par des tiers (sources externes). Cette catégorie comprend à la fois l'information qui est immédiatement disponible pour la police (par exemple, les informations du Registre national, les informations de la Banque-Carrefour des entreprises, les informations des services d'immatriculation des véhicules…) ainsi que les informations qui peuvent être récupérées de manière légale auprès de tiers (par exemple, les données des antennes des opérateurs de télécommunication) ;
- les open data sont des données qui sont librement accessibles à tous et qui peuvent être utilisées immédiatement. Les informations (disponibles gratuitement) provenant des médias sociaux, de la presse… entrent dans cette catégorie.[157]

Une unité spécialisée dans la recherche en sources ouvertes (*open-source intelligence* – OSINT) a été créée en avril 2023 à Bruxelles. Au moment de sa création, l'équipe employait près de dix personnes, et sa taille devait doubler en 2024. La cellule s'appuie sur les outils de la société allemande Maltego Technologies[158] et de Social Links,[159] originaire de Russie avant d'immigrer en Europe occidentale et aux États-Unis après l'invasion russe de l'Ukraine en 2022.

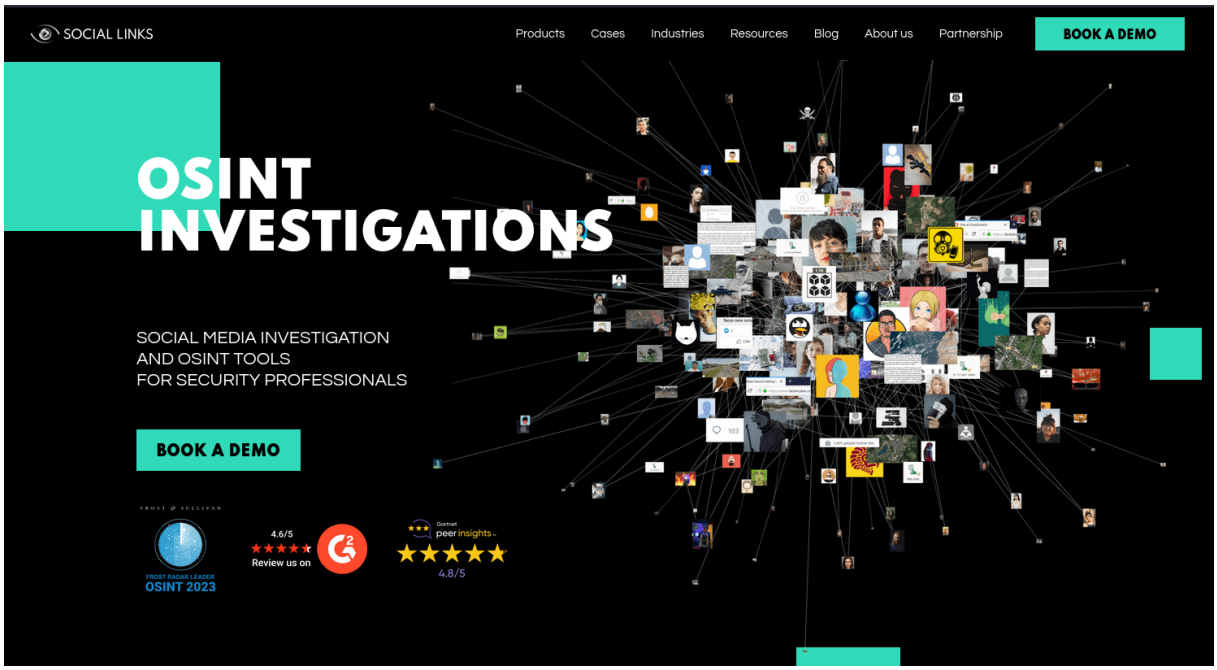

Figure 11. Page d'accueil du site de la société russe Social Links montrant un graphique social, 27/10/2023

157 Annexe H de la description du marché i-Police, p. 44
158 Maltego Technologies. URL: www.maltego.com
159 Social Links company. URL: sociallinks.io

Dans le cadre de i-Police, la division OSINT de la Police Fédérale s'apprête à mettre en œuvre la plateforme d'investigation et d'analyse de données de masse IntSight de TA9,[160] une société israélienne faisant partie du groupe Rayzone[161] dirigé par Yohai Bar-Zakai, ancien directeur adjoint de l'Unité 8200.[162] Cette dernière est « l'unité de renseignement de l'armée israélienne chargée des opérations clandestines, de la collecte de renseignements d'origine électromagnétique (SIGINT), du décryptage de codes, du contre-espionnage, de la cyberguerre, du renseignement militaire et de la surveillance ».[163] L'unité 8200 est responsable du développement de "Gospel", un système d'IA permettant de générer des cibles pour les bombardements de l'armée de l'air israélienne à Gaza, et ce à un rythme nettement supérieur à celui permis par leur détermination manuelle.[164] Le système "Gospel" a probablement contribué à faciliter le bombardement intensif de Gaza et le meurtre de Palestinien·nes lors de la récente escalade de la violence israélienne.[165]

Il est difficile de déterminer avec précision quelles autres entreprises et logiciels seront intégrés dans les solutions OSINT de i-Police. Ce qui est clair, c'est que Sopra Steria assume le rôle de maître d'ouvrage, avec le soutien de la société de conseil KPMG. Selon un article de presse, ils collaboreront avec un large éventail de sous-traitants, dont Microsoft, la société canadienne NicheRMS365[166] et les sociétés israéliennes Interionet[167] et TA9/Rayzone.[168] Un haut gradé de la Police Fédérale nous a assuré que toutes les entités tierces devront procéder aux ajustements nécessaires pour garantir la compatibilité de leurs logiciels avec les cadres juridiques belges.[169]

Un autre sous-traitant de i-Police, Interionet, est dirigé par Yair Pecht, ancien directeur général du groupe israélien NSO, spécialiste de la cyberoffensive. NSO est la société tristement célèbre pour avoir produit le logiciel espion Pegasus, qui a été utilisé contre nombre de journalistes, politicien·nes et activistes. Les antécédents controversés de NSO, marqués par des transactions avec des régimes autoritaires, ont attiré l'attention de la communauté internationale, ce qui a conduit ses dirigeants à multiplier le nombre de start-ups satellites, telles qu'Interionet.[170]

160 TA9 company. URL: www.t-a9.com
161 Rayzone Group. URL: rayzone.com
162 "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
163 "Unit 8200". *Wikipedia*. URL: wikipedia.org/wiki/Unit_8200
164 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
165 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
166 NicheRMS365 company. URL: nicherms.com/about-us
167 Interionet company. URL: www.interionet.com
168 Lars Bové & Jean-Paul Bombaerts. "La police entame une révolution digitale à 300 millions d'euros." *L'Echo*. 7/05/2022. URL: www.lecho.be/economie-politique/belgique/general/la-police-entame-une-revolution-digitale-a-300-millions-d-euros/10386480.html
169 Entretien avec un conseiller principal en R&D et en stratégie TIC au sein de la police judiciaire fédérale, 16/06/2023.
170 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?international=true&IR=T

Malgré cette tentative de laver sa réputation, Interionet fait l'objet d'une campagne de boycott. Le mouvement Boycott, Désinvestissements, Sanctions (BDS) – qui milite pour mettre fin au soutien international à l'oppression des Palestinien·nes et pour augmenter la pression sur Israël de manière à faire respecter le droit international – appelle les Belges à s'opposer au contrat entre la Police Fédérale et Interionet en raison de l'utilisation par l'entreprise de Palestinien·nes comme cobayes pour son logiciel de surveillance avant de le commercialiser à l'échelle mondiale.[171] Une telle pratique n'est pas rare, comme le révèle un livre récent du journaliste Antony Loewenstein : « le complexe militaro-industriel israélien utilise les territoires palestiniens occupés comme terrain d'essai pour l'armement et les technologies de surveillance qu'il exporte ensuite dans le monde entier, à des démocraties comme à des despotes ».[172]

Figure 12. Post Facebook du mouvement BDS, 4 novembre 2022
En description : Les Palestinien·nes appellent à faire pression pour annuler le contrat de la police belge avec la société israélienne de logiciels espions Interionet. La société cache qu'elle est basée dans l'Israël de l'apartheid et que sa technologie de reconnaissance faciale a été testée sur des Palestinien·nes. #MilitaryEmbargo #BanSpyware #IsraelOutOfMyPhone

Il est particulièrement difficile d'obtenir des informations sur les sous-traitants choisis pour i-Police. Malgré nos demandes d'accès, nos efforts pour obtenir des informations sur les sous-traitants et leurs logiciels n'ont jamais abouti. Les refus nous ont été justifiés soit par le secret industriel, soit par la crainte que la divulgation de détails sur l'architecture de la plate-forme ne compromette sa sécurité.

La députée fédérale écolo Julie Chanson n'a pas eu plus de chance lorsqu'elle a interpellé la ministre de l'Intérieur sur la question en 2023 :

> Sous le précédent gouvernement, le marché public pour la nouvelle plateforme i-police a été attribué à la société Sopra Steria. [...] Des soupçons planent cependant sur la respectabilité de certains sous-traitants de Sopra Steria. Ainsi, il me revient

171 BDS Movement. 'Don't let the Belgian police use Israeli apartheid surveillance against Belgians!'. *Facebook*. URL : www.facebook.com/BDSNationalCommittee/photos/a.129952410382961/5947579748620169
172 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

> que pourrait figurer parmi ces sous-traitants une firme israélienne sulfureuse, en lien étroit avec l'ex-société NSO Group [...]. Je suis inquiète pour la fiabilité d'une plateforme aussi stratégique qu'i-police et pour la protection des données qu'elle doit nécessairement impliquer. Pouvez-vous communiquer la liste complète des sous-traitants de Sopra Steria?[173]

Dans sa réponse, la ministre de l'Intérieur est restée évasive :

> La liste des sous-traitants ne peut pas être communiquée pour le moment [...] compte tenu des aspects de secret et de confidentialité d'une part et des aspects de sécurité de la solution i-Police d'autre part. Dans le cadre de ce marché public, les contrôles requis sur le droit d'accès et les motifs d'exclusion ont été effectués [...]. Par conséquent, il n'existait aucun motif légal d'exclure la société ou l'un de ses partenaires de la participation au présent marché public.[174]

Dans un rapport de 2017 sur les Big Data, l'autorité belge de protection des données conseillait déjà de confier au COC une mission de contrôle spécifique pour évaluer l'opportunité et l'efficacité du projet i-Police de la Police Fédérale.[175] Cependant, lorsque nous avons demandé l'avis du directeur du COC sur l'implication de sous-traitants controversés dans le projet i-Police, voici la réponse que nous avons reçue :

> On ne suit pas tous les contrats. [...] C'est de la responsabilité du ministère de l'Intérieur et de la Justice, ce sont eux qui signent les contrats en bout de course. Vu la capacité restreinte dont on dispose, on n'est pas en mesure de tout contrôler. On est capables de faire de 3 à 5 enquêtes proactives par an, pas plus. [...]
>
> Vous vous inquiétez qu'il s'agisse de firmes israéliennes, mais il n'y a pas énormément le choix, les Israéliens sont très performants. Quand je parle avec les responsables de la police judiciaire, ils disent qu'il n'y a pas beaucoup d'alternative si on veut des logiciels efficaces, seuls les Israéliens sont capables de fournir ce type de programmes. [...]
>
> [La protection des données,] c'est toujours un problème, pas seulement avec les Israéliens, déjà rien qu'avec Microsoft ! [...] Qu'est-ce qui garantit que les données ne partent pas vers les États-Unis ? La solution choisie, c'est d'imposer contractuellement que les données restent dans l'Union Européenne. Mais la NSA va-t-elle respecter ces contrats ? Rien n'est moins sûr, comme on l'a vu avec l'affaire Snowden.[176]
>
> En juin 2023, la ministre de l'Intérieur a néanmoins tenté de rassurer le Parlement, arguant que la Police Fédérale collaborait avec Europol pour évaluer ses méthodes basées sur l'IA et pour appliquer les "principes de responsabilité pour l'intelligence

173 Réponse de la ministre Verlinden à la question 1775 de Julie Chanson, députée écolo au Parlement fédéral. 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

174 Réponse de la ministre Verlinden à la question 1775 de Julie Chanson, députée écolo au Parlement Fédéral. 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

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

176 Deuxième entretien avec Frank Schuermans (COC), 11/10/2023.

artificielle" (AP4AI)[177].[178] Ces principes prétendent « constituer un cadre universel, validé empiriquement, pour l'utilisation de l'intelligence artificielle dans les secteurs de la police et de la justice, afin, fondamentalement, d'évaluer et de faire respecter l'utilisation légitime et acceptable de l'intelligence artificielle par la communauté de la sécurité intérieure ».[179] Voici quelques-uns de ces principes :

- Universalité : Chaque aspect de l'utilisation de l'IA peut être contrôlé et évalué.
- Explicabilité : Toutes les pratiques, tous les systèmes et toutes les décisions en matière d'IA peuvent être pleinement expliquées au public et aux organes de contrôle.
- Transparence : Les informations permettant d'évaluer l'utilisation de l'IA sont facilement et pleinement accessibles.
- Indépendance : Les groupes chargés de la surveillance et de l'application de la loi sont indépendants des institutions policières et des développeurs·ses d'IA.
- Compétence : Il est possible d'obliger les services répressifs à fournir les informations, les systèmes ou les personnes nécessaires pour juger de leur utilisation de l'IA.
- Engagement à fournir des preuves solides : Les services répressifs s'engagent à fournir des preuves solides pour juger de leur utilisation de l'IA.
- Pluralisme : Tous les groupes concernés et affectés par l'utilisation de l'IA ont voix au chapitre.
- Caractère exécutoire et recours : Il est possible de contraindre les services répressifs à se conformer à toutes les demandes d'amélioration de leurs pratiques en matière d'IA.

On ne sait s'il faut rire ou pleurer du décalage entre ces beaux principes et le niveau actuel de responsabilité affiché par les autorités belges. D'autant plus que tous ces programmes reposent sur des algorithmes dont le code est privé, soit protégé par la propriété intellectuelle, ce qui rend impossible la vérification de leur fonctionnement précis.

En outre, même si le code était publiquement accessible et qu'il était possible d'en discuter avec ses développeurs·ses, il ne serait peut-être pas possible d'en comprendre le fonctionnement, car de plus en plus d'algorithmes sont écrits par apprentissage automatique (*machine learning*). Les modèles d'apprentissage automatique sont souvent qualifiés de "boîtes noires", ce qui signifie qu'un modèle fonctionne comme un système opaque dont les rouages internes ne sont pas

177 Accountability Principles for Artificial Intelligence. URL: ap4ai.eu
178 Réponse de la ministre Verlinden à la question 1911 de Daniel Seneseal, député socialiste au Parlement Fédéral. 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
179 The AP4AI Principles. URL: ap4ai.eu/about/principles

clairs, tant pour les chercheurs·ses que pour les usagers·ères.[180] Le problème de la "boîte noire" peut conduire à ce que les logiciels perpétuent les préjugés et les structures de pouvoir, sans identification possible de l'origine du problème – ni de sa solution.

Enfin, les systèmes propriétaires peuvent contenir des portes dérobées (*backdoors*) permettant aux fournisseurs de logiciels d'y accéder à distance. Cette pratique est courante chez les fournisseurs israéliens, comme la Police Fédérale l'a récemment appris à ses dépens. Selon les représentants du syndicat de la police avec lesquels nous nous sommes entretenus, la police judiciaire a dû remplacer d'urgence son logiciel d'écoutes téléphoniques après avoir découvert qu'elle n'était pas seule à écouter les suspects. Au cas où vous vous demandiez « qui surveille les surveillants ? », vous avez maintenant votre réponse.

4. État d'avancement du programme "i-Police"

En août 2023, la ministre de l'Intérieur a fait rapport au Parlement fédéral des progrès accomplis dans le cadre de i-Police.[181] Il en ressort que le processus a commencé par la mise en place d'un système d'échange de données au niveau international. Au moment de la déclaration de la ministre, l'intégration du Système d'Information Schengen (SIS) était en cours de finalisation. Celle-ci devait être suivie par Europol et Interpol courant 2024.

Un deuxième projet faisait également partie du déploiement initial de i-Police : le traitement des données d'ISLP et de la BNG en vue de développer la "police guidée par le renseignement" (*Intelligence led policing* – ILP), au cœur de l'initiative. Selon l'appel d'offres :

> Le but de l'ILP consiste à recueillir ou à consulter des données (données brutes), pour les transformer en nouvelles connaissances et, sur la base de celles-ci, orienter le fonctionnement des autres domaines. Les données brutes qui sont traitées par l'ilp , peuvent provenir de différentes sources :
>
> - les données provenant du fonctionnement opérationnel de la police ;
> - les données provenant de partenaires de la police ou les données transférées par des tiers à la police (sources de données externes) ;
> - les données qui sont accessibles au public et sont reprises par la police.
>
> Ces données sont ensuite converties par l'ilp en « intelligence » ou autrement appelée « renseignement ». Ces renseignements doivent être fournis à temps, précis, de grande valeur et orientés action et sont conçus pour orienter le fonctionnement. Selon le type d'orientation, nous parlons d'intelligence opérationnelle, tactique ou stratégique.[182]

180 Lou Blouin, 'AI's mysterious 'black box' problem, explained'. *University of Michigan-Dearborn*. 6 mars 2023. URL: umdearborn.edu/news/ais-mysterious-black-box-problem-explained

181 Réponse de la ministre Verlinden à la question 1964 de Daniel Seneseal, député socialiste au Parlement Fédéral. 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

182 GPI. 2020. Annexe H de la description du marché i-Police. p. 23-24.

Une phase pilote du projet ILP a été lancée fin 2023. Elle s'est déroulée dans la province de Liège et a impliqué à la fois la police locale et la Police Fédérale. L'objectif déclaré de la phase pilote était d'identifier les points d'attention et d'amélioration avant d'aller plus loin en 2024.[183]

Cependant, des articles récents notent que le développement et la mise en œuvre du système ont rencontré quelques obstacles. Un article dans *De Tijd* affirme que la société de conseil britannique Deloitte a effectué un audit sévère de la direction informatique de la Police Fédérale. Cet audit conclut que la transformation numérique de la police n'est pas rationalisée, ce qui entraîne une approche fragmentée, et que le contrôle interne est inadéquat quant à la façon dont le personnel de la police utilise et maintient les bases de données, ce qui risque de conduire à des abus.[184] Les auteurs de l'audit ont déclaré devant le Parlement fédéral :

> Tout d'abord, pour les standards et la législation, nous avons constaté qu'il n'y a pas vraiment de gestion de l'information formalisée concernant l'exploitation opérationnelle, la sécurité et la protection des données. [...] Il n'y a pas vraiment de stratégie non plus, ni sur la sécurité de l'information, ni sur un plan d'action. [...] Le contrôle de gestion interne est limité, insuffisant dans le cadre de la gestion des informations. Il est donc important d'établir des processus de contrôle de gestion, car il s'agit de données qui relèvent strictement de la vie privée.[185]

Un autre article, paru dans *Le Soir* en 2023, signale que la Police Fédérale ne peut plus payer ses factures et que le montant total des impayés s'élève à plusieurs dizaines de millions d'euros. Le journal ajoute : « Certains consultants – notamment dans le domaine de l'IT – ne sont plus payés et commencent à réclamer leur dû avec insistance ».[186] Selon un représentant syndical avec lequel nous nous sommes entretenus, le projet i-Police fait actuellement l'objet de sérieuses révisions visant à donner la priorité à la stabilité des opérations informatiques fondamentales de la police, réduisant considérablement les aspirations initiales du projet.

Tout cela soulève des questions sur la fonction des entreprises privées qui offrent des services de consultance à une police endettée. On peut s'interroger sur le fait que le développement de i-Police ait été confié à un consortium Sopra Steria/KPMG pour ensuite confier à Deloitte le soin d'auditer le processus, ce qui a permis de conclure à une déficience de la stratégie interne. Il reste à voir si d'autres entreprises privées tireront profit de ce processus, en particulier pour l'élaboration d'une telle stratégie.

183 Réponse de la ministre Verlinden à la question 1964 de Daniel Seneseal, député socialiste au Parlement Fédéral. 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

184 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

185 Audition au Parlement Fédéral des inspecteurs de Deloitte suite à leur audit du département informatique de la Police Fédérale. *Chambre des représentants de Belgique*. Doc 55 3516/001. URL: www.lachambre.be/media/index.html?language=fr&sid=55U4143#video

186 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

Difficile de savoir à quel récit se fier : faut-il croire la police lorsqu'elle affirme utiliser des systèmes de haute technologie qui traitent toutes les données et désignent miraculeusement les criminels ? Ou devons-nous nous ranger du côté de la conclusion de Deloitte selon laquelle la police est mal organisée et dépend de logiciels obsolètes ?

Lors d'un entretien avec le directeur du COC, ce dernier a déclaré, à propos de i-Police :

> Il y a une grande différence entre ce que dit la presse et la réalité. La police n'est pas du tout aussi performante qu'on le pense. La réalité, c'est ce que décrit Deloitte. i-Police, ce sont surtout en tout cas jusqu'à l'heure actuelle des paroles. Je ne peux que le constater avec les caméras de surveillance. On annonce qu'on va mettre des caméras ANPR partout, qu'il va y avoir 10 000 nouvelles caméras, mais on n'est pas capables de connecter les 1500 caméras anpr qui sont déjà là ou de faire un système de *logging* sur ces caméras. Tout ça, c'est de la pub. Il y a un fossé énorme entre la communication et la situation sur le terrain. C'est l'exemple typique avec l'AMS (*ANPR Managed Services*), on n'est pas capables de suivre le nombre de caméras qui doivent être branchées en raison d'énormes problèmes techniques. C'est de la foutaise.[187]

Il est rassurant de savoir que le niveau de sophistication technologique de la police n'est peut-être pas à la hauteur de ses capacités proclamées. Néanmoins, le développement de i-Police devra être suivi de près, car les choses peuvent évoluer très rapidement en matière de technologie policière. Il sera également important de s'assurer qu'au cas où le projet i-Police serait abandonné, certains de ses composants les plus intrusifs ne soient pas conservés et rebaptisés.

187 Deuxième entrevue avec Frank Schuermans (COC), 11/10/2023.

Automatisation de la justice en Belgique : petits pas, mais enjeux de taille

Les algorithmes sont de plus en plus utilisés dans de nombreux pays pour anticiper les résultats d'affaires judiciaires en traitant de grandes quantités de données (lois, jurisprudence et doctrine).[188] La justice "prédictive" pourrait remplir de nombreuses fonctions, notamment celle de fournir aux personnes un aperçu de leurs chances de succès à l'issue de procédures judiciaires, ou d'aider les juges à prendre des décisions.

En Belgique, la mise en œuvre de systèmes d'aide à la décision, voire de prise de décision automatisée est considérablement entravée par le manque d'accès aux données nécessaires pour entrainer de tels outils. La dépendance persistante du système judiciaire belge aux communications analogiques rend improbable la mise en œuvre rapide de l'IA.

Toutefois, des tribunaux de droit civil ont mené des expériences de conseil juridique assistés par ordinateur[189] ; des chercheurs universitaires travaillent au développement d'ia adaptées au droit belge[190] ; et une récente loi prévoit la création d'un registre numérique centralisé des décisions de justice, ce qui permettrait théoriquement d'entrainer des algorithmes d'IA.[191] Tout cela suscite des inquiétudes quant à l'automatisation de certains aspects du processus judiciaire et, à terme, à la possibilité de décisions de justice rendues par des algorithmes, ce qui pourrait éloigner les individus de la salle d'audience, et compromettre le peu de transparence et de possibilités de contestation permis par le système actuel.[192]

Un rapport publié en décembre 2024 par la Cour des comptes fournit une analyse complète de la stratégie de transformation numérique du système judiciaire belge.[193] Il identifie des lacunes importantes dans la politique de transformation numérique. L'une des principales critiques est que, bien que le ministère de la Justice ait affecté pas moins de 140 millions d'euros spécifiquement à la numérisation en 2023, il n'a pas été en mesure de développer une stratégie unifiée et cohérente. Le rapport souligne également les manquements associés aux projets de consultance, notamment la gestion du budget, les conflits d'intérêts et l'influence commerciale.

Le développement de la justice "prédictive" ne progresse pas aussi rapidement que celui de la police. Cependant, il semble présenter un certain nombre d'écueils comparables.

188 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.

189 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

190 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

191 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.

192 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

193 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*"

Les principales observations de ce rapport sont brièvement récapitulées ci-dessous avant d'ouvrir la discussion sur les façons d'envisager une approche critique du développement de l'intelligence artificielle dans la police. Nous pensons qu'il est nécessaire d'imposer des obligations en matière de transparence, de responsabilité et d'équité, mais surtout une interdiction totale de la police "prédictive".

1. Résumé

I. En Belgique, les **zones de police locale** jouissent d'une autonomie importante, ce qui se traduit par des situations extrêmement variées à travers le pays.

En l'absence de politiques transparentes, il est impossible d'obtenir une vue d'ensemble de leurs activités. On sait néanmoins que de nombreuses zones de police cartographient des "points chauds" en vue de guider leurs patrouilles, et que certaines zones de police revendiquent fièrement la mise en œuvre de méthodes de police "prédictive", comme Westkust, Zennevallei et Anvers. Cette dernière, l'une des plus grandes zones de police du pays, est à la pointe de l'automatisation. FOCUS, l'application mobile développée en interne à Anvers, donne aux policiers de terrain un accès direct à toute une série de données. Elle a été généralisée à tout le pays et devrait constituer l'interface principale pour accéder aux fonctionnalités du projet fédéral "i-Police".

II. Les systèmes de police "prédictive" s'appuient en premier lieu sur les **bases de données policières.**

Cependant, en Belgique, ces bases de données sont nombreuses, mal gérées et ne respectent souvent pas le cadre légal. Les bases de données policières ont déjà de sérieuses répercussions sur les individus, dans la mesure où les inexactitudes et les classifications injustes peuvent entraîner des fouilles injustifiées, des contrôles de sécurité renforcés (notamment dans les aéroports) ou compromettre l'avenir professionnel des personnes fichées. Les informations erronées portent souvent atteinte à la réputation et aux moyens de subsistance des personnes.

En outre, la surveillance policière en général et notamment du travail du sexe et des "bandes" urbaines, ainsi que les politiques de lutte contre la radicalisation, ciblent de manière disproportionnée les groupes déjà marginalisés et renforcent les inégalités structurelles existantes. Sans contre-mesures sérieuses, l'automatisation du maintien de l'ordre ne pourra qu'exacerber ces problèmes, d'autant plus que toute contestation ou demande de réparation est rendue difficile voire impossible par l'absence de droits d'accès direct et de voies de recours significatives.

III. i-Police est un plan lancé par la Police Fédérale en vue de mettre à niveau son infrastructure informatique largement obsolète.

Ce projet de 300 millions d'euros vise aussi à analyser et recouper automatiquement toutes sortes de données, y compris les bases de données des polices locales, fédérale et internationale, mais aussi les images de vidéosurveillance et des sources externes. Les données (analysées ou brutes) sont ensuite censées être largement mises à la disposition des agents sur le terrain comme dans les commissariats.

1. Le programme i-Police suscite un certain nombre de préoccupations, notamment en ce qui concerne l'utilisation d'algorithmes opaques ou la centralisation de grandes quantités de données – de qualité variable – dans un **"lac de données"** (*data lake*).

Ce "lac de données" risque de brouiller la distinction entre les informations vérifiées ou non. En informatique, le principe *"garbage in, garbage out"* (déchets à l'entrée, déchets à la sortie) indique que des données d'entrée de mauvaise qualité ne sauraient produire des résultats fiables. C'est précisément ce que l'on peut craindre avec le développement de la police "prédictive" en Belgique.

2. i-Police intégrera des images de **vidéosurveillance**.

Ce point suscite plusieurs inquiétudes, car la Belgique a été prise en flagrant délit de violation de son propre cadre légal à de nombreuses reprises. Qu'il s'agisse de l'utilisation de la reconnaissance faciale à l'aéroport de Zaventem ou de l'emploi du logiciel Clearview AI, la police belge semble préférer accueillir les possibilités offertes par les nouvelles technologies plutôt que de se conformer aux exigences minimales en matière de droit. À l'heure où le gouvernement prévoit de mettre en place des caméras ANPR dans tout le pays et de légaliser la reconnaissance faciale, il y a des raisons de s'inquiéter et de réagir.

3. Le programme i-Police prévoit d'utiliser et d'analyser des sources externes, une pratique connue sous le nom d'**open-source intelligence** (OSINT). S'il est difficile de clarifier quelles seront précisément les entreprises qui participeront au projet et les logiciels qu'elles utiliseront, le principal contractant de i-Police est Sopra Steria, en partenariat avec la société de conseil KPMG. Quoi qu'il en soit, l'analyse des données dépendra d'algorithmes au fonctionnement opaque, fournis par des contractants privés et étrangers dont les pratiques sont éthiquement discutables.

4. Néanmoins, ces dernières années, la Belgique a rencontré des **obstacles** dans la mise en œuvre de i-Police.

Un audit externe a révélé que la transformation numérique de la police était désordonnée et qu'il y avait un manque de contrôle interne, de sécurité, et

de mesures de protection de la vie privée, ce qui est particulièrement inquiétant lorsqu'il s'agit de traiter quantité d'informations aussi confidentielles. Enfin, la Police Fédérale est confrontée à des difficultés financières, ses dettes s'élevant à plusieurs dizaines de millions d'euros. Il est donc probable que le projet i-Police fasse l'objet de révisions, l'accent étant mis sur la stabilité des opérations de base.

2. Discussion

La numérisation et l'automatisation dans les domaines de la police et de la justice en Belgique sont à géométrie variable. L'adoption de nouvelles technologies est bien plus avancée dans la police que dans la justice. Ces développements, à différents rythmes, soulignent la nécessité de rester sur nos gardes. Les deux contextes soulèvent des inquiétudes quant aux violations potentielles des droits fondamentaux et au renforcement de dynamiques de discrimination et de criminalisation. La vigilance est de mise pour anticiper les processus de numérisation et d'automatisation.

Tout d'abord, les systèmes "prédictifs" sont connus pour cibler et discriminer de manière disproportionnée les groupes marginalisés, renforçant ainsi les inégalités structurelles existantes. Des 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.

Le manque de transparence, de responsabilité et de droit de recours effectif aggrave ces problèmes. Les systèmes d'IA "prédictifs" opèrent derrière des 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 ces "boîtes noires" et de contester leurs décisions opaques.[194]

En outre, les systèmes "prédictifs" portent atteinte aux principes fondamentaux comme le droit à la vie privée, à la libre circulation et à un procès équitable ; la liberté d'association et l'égalité de traitement devant la loi. Des lieux, des individus, ou des groupes sont étiquetés comme "menaces potentielles", ce qui entraîne des mesures punitives, telles que des privations de liberté injustifiées. Cela érode le principe essentiel de présomption d'innocence et pose un grave risque d'erreur judiciaire.

Entretemps, ni analyse d'impact sur les droits humains ni analyse coûts-bénéfices de base n'ont été menées en préparation des systèmes "prédictifs" belges. L'absence de toute évaluation préalable du potentiel de nuisance de ces systèmes soulève des doutes quant à l'efficacité, la proportionnalité, la nécessité et les conséquences à long terme de ces mesures. Il serait impératif de s'interroger sur les impacts de la police "prédictive" avant de l'adopter aveuglément.

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

À la question de savoir si la police “prédictive” devrait être autorisée en Belgique, le directeur du COC a répondu :

> C’est une question très difficile. C’est avant tout une question pour le législateur et le parlement [...]. À ce stade, je suis très réticent à répondre par l’affirmative à cette question. Non pas tant en raison du principe selon lequel cela ne devrait pas être possible, mais en raison de l’expérience quotidienne que nous avons ; dans le cadre de notre travail quotidien, nous constatons qu’il y a un énorme problème d’exactitude des données policières. Même aujourd’hui, sans le *big data*. Et c’est précisément parce que cela constituerait la base de tous les systèmes de profilage.[195]

Actuellement, des discussions sont menées entre la société civile, les élu·es et les universitaires sur la réglementation de l’IA, afin de minimiser son potentiel de nuisance, y compris dans le cadre du maintien de l’ordre. En Belgique, un chercheur de la KU Leuven, Thomas Marquenie, propose une série de lignes directrices pour réglementer l’IA. Il souligne

- l’impératif de se conformer à la loi sur la protection des données, notamment par le recours systématique à des analyses d’impact sur la protection des données (AIPD) ;
- la nécessité de restreindre le profilage et de limiter l’utilisation de données sensibles ;
- l’importance d’avoir toujours un “humain dans la boucle” pour faire respecter les principes de responsabilité et d’imputabilité ;
- la valeur de la transparence publique : les autorités devraient informer les citoyens et partager des informations sur les outils qu’elles utilisent et les données qu’elles traitent ;
- que le recours à l’ia doit être limitée à des objectifs, des profils et des situations bien définies ;
- que l’utilisation de l’IA devrait toujours reposer sur une base légale et la police devrait consulter l’organe de contrôle (COC) avant de mettre en œuvre de nouveaux outils.[196]

Les propositions de Marquenie semblent raisonnables et l’on pourrait en ajouter quelques-unes, telles que des fichiers de police fiables, des pratiques rigoureuses de minimisation des données et des audits réguliers, en tant qu’exigences minimales pour le développement de toute “solution fondée sur les données”.

Toutefois, ces propositions réglementaires ne vont pas assez loin pour tenir compte des préjudices causés par le maintien de l’ordre fondé sur les données. Le présent rapport a identifié les problèmes structurels de racisme, d’islamophobie et de classisme dans la police belge. Ces enjeux sont systémiques et ne peuvent être résolus par la seule application de quelques règles.

195 Entrevue avec Frank Schuermans (COC), 17/02/2023.

196 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)*. 17/06/2022. URL: vaia.be/files/cursusmateriaal/presentaties/220617-3-Thomas-Marquenie.pdf

Il est faux de croire que la police belge respectera dûment le cadre juridique autour de l'IA. En effet, la police belge s'est trop souvent illustrée par le non-respect des exigences minimales en matière de gestion des données. Les rapports du COC sur la reconnaissance faciale à l'aéroport de Bruxelles, sur Clearview AI et sur la BNG démontrent que la Police Fédérale viole régulièrement la loi. Cela met en évidence des problèmes structurels qui ne peuvent être résolus immédiatement. En outre, l'exactitude des données policières laisse bien souvent à désirer. Dans un tel contexte, tout espoir d'une utilisation équitable des outils de police "prédictive" est illusoire.

En outre, la police "prédictive" repose sur l'hypothèse que certains lieux ou individus sont intrinsèquement enclins à des activités criminelles. Ces hypothèses reposent sur des théories criminologiques qui manquent de base empirique et simplifient à l'excès la nature complexe des causes de la criminalité et de la délinquance.

Il semble donc raisonnable de s'opposer résolument au développement d'outils de police "prédictive" en Belgique. Comme le conclut un récent mémoire sur le projet i-Police :

> Il a été évoqué ci-avant les solutions existantes afin de limiter la casse. Cependant il ne faut pas se leurrer, ces solutions apparaissent finalement comme des bouées de sauvetage là où c'est le navire qu'il faut empêcher de couler. L'usage de la police prédictive est un non-sens pour plusieurs raisons dont certaines ont été évoquées au fil de ce mémoire. Pire qu'un non-sens, elle constitue à plein d'égards un danger qu'il ne faut sous-estimer en raison de l'apparence faussement neutre attribuée aux technologies. Le temps, l'énergie et l'argent investis dans ces outils auraient pu trouver un placement plus rentable dans l'éducation, la police de proximité ou dans la lutte contre les inégalités qui sont des moyens durables de lutter contre la délinquance. Certains me traiteront d'utopiste mais où se trouve réellement l'utopie quand on prétend pouvoir prédire le crime ?[197]

L'antagonisme est clairement explicité par le Comité permanent de la police locale (CPPL), l'organisation coupole des zones de police locale. Dans le document *Horizon 2025*, le Comité déclare :

> En fait, malgré toutes les transformations de soutien en matière d'ILP (i-Police, FOCUS, ANPR...), nous n'en sommes encore qu'à la veille de ladite révolution. Les futures possibilités sont infinies avec comme summum l'évolution vers une "predictive policing" sur la base de "big data" et de "datamining". Tous les jours, nous nous heurtons aux limites des concepts "vie privée" et "droits de l'homme". Le débat sur la vie privée doit être mené d'urgence en ayant pour principe de base : "L'Exploitation de l'information et de la technologie pour renforcer la qualité de vie et la sécurité du citoyen !"[198]

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

198 CPPL, 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

À la lumière de ces préoccupations pressantes, il est impératif que la Belgique interdise l'utilisation de systèmes de police "prédictive" et de prise de décision automatisée en matière de justice. En interdisant ces systèmes, la Belgique peut faire un pas important vers la construction d'une société plus équitable, plus juste et plus démocratique. C'est l'occasion de réaffirmer un engagement à défendre les droits fondamentaux, à promouvoir l'égalité et à maintenir vivants les principes de justice et de responsabilité. En conclusion, la police "prédictive", telle qu'elle existe en Belgique, est loin d'être une entreprise responsable, efficace ou éthique. Il est primordial que nous remettions en question son adoption, en nous engageant résolument à protéger nos droits et notre liberté. Il nous incombe d'élever la voix pour nous opposer à la police "prédictive". Une telle interdiction serait un pas vers un avenir où la justice et l'égalité ne sont pas compromises par l'innovation technologique. C'est l'affirmation que les droits et le bien-être des personnes sont primordiaux et que nous nous opposons fermement à toute technologie qui porte atteinte à ces principes.

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 TIC
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