LIÈGE université Library

https://lib.uliege.be https://matheo.uliege.be

Maintenir l'ordre à l'ère des caméras dotées de capacités algorithmiques : Perceptions des fonctionnaires dirigeants de police locale belges sur les enjeux, défis et pratiques de ces nouvelles technologies

Auteur : Chavée, Chloé
Promoteur(s) : Seron, Vincent
Faculté : Faculté de Droit, de Science Politique et de Criminologie
Diplôme : Master en criminologie à finalité spécialisée en criminologie interpersonnelle
Année académique : 2025-2026
URI/URL : http://hdl.handle.net/2268.2/26497

Avertissement à l'attention des usagers :

Tous les documents placés en accès ouvert sur le site le site MatheO sont protégés par le droit d'auteur. Conformément aux principes énoncés par la "Budapest Open Access Initiative"(BOAI, 2002), l'utilisateur du site peut lire, télécharger, copier, transmettre, imprimer, chercher ou faire un lien vers le texte intégral de ces documents, les disséquer pour les indexer, s'en servir de données pour un logiciel, ou s'en servir à toute autre fin légale (ou prévue par la réglementation relative au droit d'auteur). Toute utilisation du document à des fins commerciales est strictement interdite.

Par ailleurs, l'utilisateur s'engage à respecter les droits moraux de l'auteur, principalement le droit à l'intégrité de l'oeuvre et le droit de paternité et ce dans toute utilisation que l'utilisateur entreprend. Ainsi, à titre d'exemple, lorsqu'il reproduira un document par extrait ou dans son intégralité, l'utilisateur citera de manière complète les sources telles que mentionnées ci-dessus. Toute utilisation non explicitement autorisée ci-avant (telle que par exemple, la modification du document ou son résumé) nécessite l'autorisation préalable et expresse des auteurs ou de leurs ayants droit.

LIÈGE université
Droit, Science Politique & Criminologie

Maintenir l'ordre à l'ère des caméras dotées de capacités algorithmiques :

Perceptions des fonctionnaires dirigeants de police locale belges sur les enjeux, défis et pratiques de ces nouvelles technologies

Travail de fin d'études présenté en vue de l'obtention du diplôme de Master en Criminologie, à finalité spécialisée en criminologie interpersonnelle

Chloé Chavée

Année académique : 2025-2026

Promoteur : Vincent Seron

Professeur au Département de Criminologie,
Université de Liège

Résumé

Le développement de l'intelligence artificielle (IA) occupe une place croissante dans notre société et influence progressivement les pratiques des services de police, notamment en matière de sécurité publique et de maintien de l'ordre. Cette recherche s'intéresse à l'intégration d'outils tels que des caméras dites augmentées au sein des zones de police locale en Belgique et aux enjeux qu'elles soulèvent. L'étude repose sur une méthodologie qualitative fondée sur des entretiens semi-directifs réalisés auprès de fonctionnaires de police exerçant principalement des fonctions dirigeantes. Ces outils sont globalement considérés comme nécessaires et appelés à se développer progressivement dans les pratiques policières, notamment en raison de leur potentiel en matière de prévention, d'analyse et de gestion de l'espace public. Une attention particulière est portée aux défis structurels, organisationnels et opérationnels que posent ces technologies ainsi qu'aux inégalités existantes entre les zones en matière d'accès et de gestion de ces outils. Des interrogations surviennent également concernant la protection des droits fondamentaux. Le cadre juridique belge est perçu comme insuffisamment adapté aux évolutions rapides de l'IA, favorisant une approche prudente quant à son intégration dans les pratiques policières. Ainsi, cette recherche souligne la nécessité d'un encadrement juridique, organisationnel et éthique permettant de concilier innovation technologique, réalités de terrain et garanties démocratiques.

Mots clés : IA – caméras – vidéosurveillance – algorithmes – caméras augmentées – police locale – ordre public – sécurité – enjeux – défis – droits fondamentaux

Abstract

The development of artificial intelligence (AI) is playing an increasingly significant role in our society and is gradually influencing police practices, particularly in the areas of public safety and law enforcement. This research examines the integration of tools such as so-called 'augmented' cameras within local police forces in Belgium and the issues they raise. The study employs a qualitative methodology based on semi-structured interviews with police officers, primarily those in managerial roles. These tools are generally considered necessary and are expected to become increasingly integrated into police practices, particularly due to their potential for prevention, analysis and the management of public spaces. Particular attention is paid to the structural, organisational and operational challenges posed by these technologies, as well as to existing inequalities between areas in terms of access to and management of these tools. Questions also arise regarding the protection of fundamental rights. The Belgian legal framework is seen as ill-suited to the rapid developments in AI, leading to a cautious approach to its integration into police practices. This research therefore highlights the need for a legal, organisational and ethical framework that can reconcile technological innovation, practical realities on the ground and democratic safeguards.

Keywords : AI – cameras – CCTV – algorithms – augmented cameras – local police – public order – security – issues – challenges – fundamental rights

Table des matières

Résumé 2
Abstract 2
Remerciements 6
1. Introduction 7
2. Revue de la littérature 8
2.1 La technicisation des pratiques policières 8
2.2 Comprendre l'intelligence artificielle 8
2.2.1 Machine Learning et Deep Learning 9
2.2.2 Big data et qualité informationnelle 10
2.3 Applications de l'IA dans la sécurité publique 10
2.3.1 IA et police : vers une transformation structurelle 10
2.3.2 IA, prévention et sécurité publique 11
2.3.3 Human-in-the loop et nécessité d'adaptabilité 11
2.4 Caméras et algorithmes 12
2.4.1 Définition et distinction entre « caméras biométriques » et « caméras augmentées » 12
2.4.2 Fonctionnement des caméras augmentées et intégration des dispositifs dans les pratiques policières 13
2.4.3 Exemple d'utilisation des caméras augmentées et de la reconnaissance faciale 13
2.5 Limites et défis des technologies liées aux caméras associées aux algorithmes 15
2.5.1 Risques de biais et discriminations 16
2.5.2 Manque de transparence dans les processus décisionnels algorithmiques 16
2.5.3 Atteintes potentielles aux libertés et droits fondamentaux : responsabilité, transparence et explicabilité comme gage de confiance 17
2.5.4 Défis technique liés à l'intégration des outils d'IA 18
2.6 Cadre juridique relatif à l'utilisation des caméras par les services de police 18
2.6.1 Loi du 21 mars 2007 réglant l'installation et l'utilisation des caméras de surveillance (2007, modifiée en 2018) – Législation nationale belge 19
2.6.2 Loi du 5 août 1992 sur la fonction de police (LFP) - Législation nationale belge 19
2.6.3 Loi du 30 juillet 2018 sur la protection des personnes physiques à l'égard du traitement des données – Législation nationale belge 19
2.6.4 Le Règlement général sur la protection des données (RGPD) – Législation européenne 19
2.6.5 La directive (UE) 2016/680 du 27 avril 2016 – Législation européenne 19
2.7 Cadre juridique relatif à l'utilisation de caméras augmentées 20
2.7.1 Le Règlement européen sur l'intelligence artificielle 2024 (IA Act) : un cadre européen fondé sur les risques – Législation européenne 20
2.8 Contrôle des pratiques policières 22
2.8.1 Autorité de protection des données (APD) 22

2.8.2 Organe de contrôle de l'information policière (COC) 22
2.8.3 Le comité permanent de contrôle des services de police (Comité P) 22
2.9 État des lieux des dispositifs caméras en Belgique 23
2.9.1 Une expansion continue des caméras : du réseau classique à la vidéo intelligente 23
2.9.2 Un déploiement territorial inégal et corrélé à des facteurs socioéconomiques 23
2.9.3 Introduction progressive de la vidéo intelligente : l'exemple de BriefCam 23
2.9.4 Débats actuels et projets controversés en Belgique 24
3. Méthodologie 24
3.1 Type de recherche 24
3.2 Échantillon et stratégie d'échantillonnage 25
3.3 Organisation de l'entretien 26
3.4 Outil de récolte 27
3.5 Positionnement de la chercheuse 27
4. Résultats 27
4.1 Gouvernance, cadre normatif et conditions de légitimité 27
4.1.1 Une gouvernance « multicouche » et un cadre mouvant 27
4.1.2 La recherche d'un encadrement conforme au principe de « privacy by design » 28
4.1.3 La traçabilité et le contrôle comme garanties de responsabilisation 29
4.1.4 Transparence, communication et acceptabilité des dispositifs 29
4.1.5 Vers une harmonisation des pratiques et des cadres d'utilisation 30
4.2 Les usages et finalités de l'utilisation des caméras augmentées dans les pratiques policières 30
4.2.1 Les caméras augmentées comme outils de gestion de l'ordre public 30
4.2.2 Un soutien opérationnel durant les interventions policières 30
4.2.3 L'accélération de l'exploitation des images dans les enquêtes 31
4.2.4 Des effets préventifs perçus comme relatifs et contextuels 32
4.2.5 L'intelligence artificielle comme outil de rationalisation organisationnelle 32
4.3 Limites techniques et défis opérationnels de l'intégration de caméras augmentées 33
4.3.1 Des contraintes financières et infrastructurelles importantes 33
4.3.2 Des contraintes humaines et organisationnelles persistantes 33
4.3.3 Les limites liées à la qualité des données et au paramétrage des systèmes 34
4.3.4 Le maintien de l'humain au cœur du processus décisionnel 34
4.3.5 Dépendance aux infrastructures et impact environnemental 34
4.4 Droits fondamentaux, risques de dérives et rapports de pouvoir 35
4.4.1 Les risques perçus pour les droits fondamentaux 35
4.4.2 L'acceptabilité sociale comme enjeu politique et sociétal 36
4.4.3 Les usages perçus comme disproportionnés ou inacceptables 36
4.4.4 Dépendance technologique, souveraineté et rôle du secteur privé 36

5. Discussion 37
Forces et limites de l'étude 40
Perspectives futures 41
6. Conclusion 41
Bibliographie 43
Ouvrages 43
Contribution à un ouvrage collectif 43
Articles de revue 43
Littérature grise 48
Textes juridiques 49
Sites internet 51
Thèses / Mémoires 53
Notes de cours 53
Annexes 54
Annexe 1 : Tableau récapitulatif des participants 54
Annexe 2 : Guide d'entretien semi-directif 55
Annexe 3 : Formulaire de consentement 58
Annexe 4 : Arbre thématique 62
Annexe 5 : Schéma représentant les relations hiérarchiques entre l'intelligence artificielle, l'apprentissage automatique et l'apprentissage profond 66

Remerciements

Au terme de ce travail de fin d'études, je tiens à adresser mes remerciements à celles et ceux qui, de près ou de loin, ont contribué à son aboutissement. Ce travail s'est construit dans la durée. Il est le fruit de rencontres, d'échanges et de soutiens qui ont jalonné mon parcours.

Je souhaite exprimer ma profonde gratitude à mon promoteur, Monsieur Seron, pour son accompagnement, sa patience, sa disponibilité et sa bienveillance tout au long de l'évolution de ce travail de fin d'études, malgré le temps que ce dernier a nécessité. Ses conseils et sa rigueur ont été déterminants pour structurer ma réflexion et mener ce projet à terme.

Je remercie également l'ensemble des personnes rencontrées dans le cadre de cette recherche, qui ont accepté de me consacrer du temps et de me partager leur expérience. Leurs propos, leurs nuances et parfois leurs questionnements ont nourri mon analyse et ont contribué à enrichir mes réflexions tant sur le plan universitaire que professionnel.

Une pensée toute particulière va à mes collègues du Pep's pour leur compréhension, leur solidarité et leurs encouragements. Leur soutien m'a permis de concilier au mieux les exigences de ce travail avec mes responsabilités professionnelles.

Je remercie enfin ma famille et mes proches pour leur patience, leur présence, leur soutien constant et leurs précieuses relectures. Leur confiance et leurs encouragements ont été un appui précieux pour moi tout au long de ce parcours.

1. Introduction

Nous ne sommes pas sans savoir que la technologie est en perpétuelle évolution, surtout au XXI ème siècle, où cette dernière bat son plein. Nous nous approprions les technologies numériques à une vitesse exponentielle (Lafrate, 2018). Parmi ces nouvelles technologies, nous retrouvons l'intelligence artificielle (IA) qui s'impose comme l'un des moteurs majeurs d'évolution des sociétés contemporaines. Le développement des technologies numériques, le nombre croissant de données massives (Big Data) ainsi que les progrès en apprentissage automatique ont contribué à l'intégration de l'IA dans de nombreux domaines, notamment dans celui de la sécurité publique (Georges, 2019 ; Lafrate, 2018 ; Le Pollotec, 2018). Selon Villani (2019), l'IA impacte l'ensemble des secteurs sociaux et institutionnels, que ce soit au niveau de l'économie, de la justice, de la santé, de la défense ou bien de l'action policière. L'IA englobe donc un large éventail de disciplines et inclut une grande diversité d'algorithmes (Besse et al., 2018). L'IA va avoir un impact clair sur le fonctionnement des forces de l'ordre en leur offrant des outils novateurs ainsi que de nouvelles possibilités pour renforcer les capacités en matière de protection de la sécurité publique. En effet, nous pouvons nous attendre à ce que l'IA révolutionne la manière dont les autorités policières analysent les ensembles de données complexes, optimise les méthodes de police scientifique et développe des canaux de communication sécurisés (Europol, 2024). D'autant plus que les services de police sont confrontés à des formes de criminalité qui exploitent les nouvelles technologies et investissent l'espace numérique (Nouth et al., 2019 ; Faqir, 2023).

Selon Faqir (2019), les mécanismes d'intelligence artificielle reposant notamment sur des algorithmes d'apprentissage profond et d'apprentissage automatique, peuvent être mobilisés, entre autres, pour détecter des anomalies au sein des foules à partir des systèmes caméras. Par ailleurs, il est établi que ces derniers renforcent les capacités de surveillance en temps réel. Dans ce contexte, les caméras dans lesquelles sont intégrés des algorithmiques constituent un enjeu émergent majeur pour les autorités policières puisque l'intégration d'algorithmes d'apprentissage automatique permet de détecter, classifier ou analyser automatiquement des comportements, des situations ou des objets (CNIL, 2022). Ce type de technologie est progressivement introduit dans les pratiques policières, notamment dans les contextes urbains caractérisés par une forte densité de population et des enjeux sécuritaires multiples. Cela s'explique par le fait que l'automatisation des analyses d'images permet un traitement plus rapide des flux vidéo, une détection plus précoce d'évènements suspects ainsi qu'une optimisation du travail opérationnel des forces de l'ordre (Berckmans, 2024 ; Laurier, 2024 ; Lastrayoli, 2024 ; Javed & Noman, 2012). Toutefois, cette évolution technologique soulève des questions fondamentales relatives aux droits et libertés des citoyens notamment sur la protection des données personnelles, le respect de la vie privée, la légitimité démocratique de ces pratiques et sur les risques de discrimination liées aux biais algorithmiques (Besse et al., 2018 ; Castets-Renard, 2019 ; Barocas & Selbst, 2016). Il est donc important de veiller à trouver un équilibre entre innovation, impact sociétal et implications éthiques (Europol, 2024). En parallèle, l'Union Européenne et les États membres ont progressivement élaboré des cadres réglementaires visant à encadrer ces usages, notamment à travers le Règlement Général sur la Protection des Données (RGPD), la Directive 2016/680 et, plus récemment, l'IA Act.

En Belgique, ces technologies s'inscrivent dans un paysage sécuritaire en pleine évolution. L'augmentation du nombre de caméras, le développement de Centres de Supervision Urbain (CSU) dans certaines zones de police locales, ainsi que les expérimentations locales d'outils comme BriefCam témoignent d'une dynamique croissante d'intégration des caméras, le cas échéant intelligentes, dans les politiques publiques de sécurité (Debailleul, 2023, Bocquet, 2021). Toutefois, leur déploiement n'est pas uniforme et s'articule avec des enjeux socioéconomiques et géographiques qui nécessitent une analyse approfondie (De Keersmaecker & Debailleul, 2016 ; Debailleul, 2023).

2. Revue de la littérature

2.1 La technicisation des pratiques policières

Selon Benoît Dupont (2004), ce phénomène n'est pas récent et ses premières manifestations remontent à la fin du XIXème siècle, avant de connaître une intensification significative avec la transition des sociétés post-industrielles vers l'ère des nouvelles technologies. L'auteur relève trois vagues d'innovations successives ayant modifiées la police au cours du XXème siècle. La première vague s'articule autour de la « motorisation des forces de police » et de la naissance d'une police scientifique. Ensuite, la seconde est la « démocratisation des moyens de communication du public avec la police ». Cela se manifeste par la généralisation des téléphones dans les foyers et le développement d'outils de communication intra-organisationnelle comme la radio transmission et les systèmes CAD (Computer Aided Dispatch), érodant quelque peu « la dimension préventive du travail policier » (Dupont, 2004 p. 111). Enfin, la troisième vague est celle de l'intégration de l'informatique au sein des techniques policières. Il peut, par exemple, s'agir de la construction de bases de données ou d'un site internet, de l'accès aux informations depuis des terminaux mobiles etc. Pour Dupont (2004), cette transformation des services de police serait « le reflet d'une tendance générale observable dans les sociétés modernes, mais elle résulte également d'une logique industrielle et économique qui la dépasse » (Dupont, 2004 p. 112).

L'institution que constitue la police est sans cesse confrontée à une délinquance capable de s'adapter aux nouvelles conditions de son environnement (Dupont, 2004). Les services de police tentent eux aussi de se tourner vers de nouvelles technologies (Davies & Krame, 2023 ; Van Biervliet et al., 2025 ; Europol, 2024). En Belgique, depuis plusieurs années, nous observons le développement de nouvelles technologies, notamment liées aux caméras, avec des outils tels que les caméras ANPR capables de lire et analyser des plaques d'immatriculation (Trotta & Donnay, 2017), des bodycams portées par les agents de police lors de leurs interventions (Police Locale Uccle / W-B / Auderghem, (*n. d.*) ; Verly, 2025), des drones utilisés notamment dans l'analyse des scènes de crimes et des accidents de la route majeurs, la recherche de personnes disparues, la localisation de suspects, l'appui aux équipes chargées de la surveillance de manifestation d'autres évènements publics (embouteillages, gestion de foule, trouble à l'ordre public, etc.) (Police Locale Gaume, *n.d.*). D'autres types de caméras sont aussi développés telles que des caméras embarquées, à vision thermique, nocturnes ou bien encore à 360 degrés. Nous observons aussi l'apparition des technologies biométriques (Van Biervliet et al., 2025) recourant, pour certaines à de l'intelligence artificielle (IA). Selon le rapport de l'Observatoire du laboratoire d'innovation d'Europol (2024), l'IA s'inscrit comme un vecteur de transformation majeur des forces de l'ordre en mettant à disposition des outils innovants susceptibles de renforcer les capacités en matière de sécurité publique. En effet, ces technologies offrent de nouvelles possibilités en matière d'analyse de volumes importants de données, d'optimisation des méthodes médico-légales et de sécurisation des communications. Toutefois, il est à noter que les ressources financières des services de police semblent déterminantes dans le processus d'adoption d'une nouvelle technologie (Dupont, 2004).

2.2 Comprendre l'intelligence artificielle

L'intelligence artificielle (IA) constitue une discipline scientifique mobilisant des méthodes computationnelles permettant à des systèmes techniques d'accomplir des tâches traditionnellement associées aux capacités humaines telles que la perception, le raisonnement ou la prise de décision (Le Pollotec, 2018 ; Haiech, 2020). Si la littérature propose une multiplicité de définitions, plusieurs éléments consensuels peuvent être retenus afin de délimiter le concept pour les besoins de notre recherche.

Selon Villani (2019), le terme d'IA renvoie à toute solution algorithmique capable d'exécuter des tâches complexes et évolutives, nécessitant la prise en compte de multiples paramètres. De manière

complémentaire, Haiech souligne que l'IA vise à « construire des dispositifs stimulant les processus cognitifs humains ce qui conduit à définir l'intelligence comme la capacité à capter des informations, les stocker, les traiter et utiliser le résultat de ces traitements pour éventuellement déclencher une action » (2020, p. 919). Dans cette même perspective, Le Pollotec (2018) décrit l'IA comme « une discipline scientifique qui vise à simuler, en les décomposant, les différentes facultés cognitives humaines sur des ordinateurs via des algorithmes » telle que le raisonnement logique, la reconnaissance d'objets sur des images, la reconnaissance des sons et des tonalités, le langage naturel, etc. (Le Pollotec, 2018, p. 75). Les algorithmes peuvent être définis comme « une suite d'opérations ou d'instructions permettant d'obtenir un résultat » (Bertail et al., 2019, p. 7).
Sur le site officiel du parlement européen, nous retrouvons la définition suivante : « L'IA désigne la possibilité pour une machine de reproduire des comportements liés aux humains, tels que le raisonnement, la planification et la créativité. L'IA permet à des systèmes techniques de percevoir leur environnement, gérer ces perceptions, résoudre des problèmes et entreprendre des actions pour atteindre un but précis. L'ordinateur reçoit des données (déjà préparées ou collectées via ses capteurs) les analyse et réagit. Les systèmes dotés d'IA sont capables d'adapter leurs comportements (plus ou moins) en analysant les effets produits par leurs actions précédentes, travaillant de manière autonome. » (Parlement européen, 2020). Cette dernière définition rejoint celles proposées par les auteurs ci-dessus, tout en y intégrant les différents éléments clés. Elle servira donc de cadre conceptuel au sein de cette recherche.

2.2.1 Machine Learning et Deep Learning

La distinction entre « IA forte » et « IA faible » est couramment mobilisée dans la littérature. La première fait référence à une machine pouvant faire preuve de conscience ou d'intention. Actuellement, elle relève de la spéculation scientifique (Lafrate, 2018). La seconde désigne des systèmes capables de réaliser des tâches spécifiques à l'aide d'algorithmes auto-apprenants (Lafrate, 2018). Ces systèmes reposent sur des techniques d'apprentissage automatique (Machine Learning), qui consistent à entrainer des algorithmes à partir d'un grand volume de données afin qu'ils puissent identifier des régularités et résoudre certains types de problèmes. Comme le souligne Castets-Renard (2019, p. 2), ce processus « implique la mise en œuvre de techniques par lesquelles l'algorithme « apprend » une multitude de scénarios à partir d'une masse de données ».

Bien que ces systèmes présentent une capacité d'apprentissage autonome, ils restent tout de même dépendants d'une intervention humaine, notamment pour la conception des algorithmes ainsi que le choix et la structuration des données (Poullet, 2021). Toutefois, une fois déployés, ils sont en mesure, à partir des données qu'ils ont reçues, d'identifier de nouvelles corrélations, de prendre des décisions ou de formuler des prédictions. Par conséquent, le système peut progressivement s'éloigner des intentions initiales définies par son concepteur (Poullet, 2021). Dans ce contexte, « les algorithmes d'apprentissage automatique jouent un rôle crucial dans l'analyse et l'interprétation de ces données, en particulier lorsque l'analyse humaine serait trop lente ou inefficace » [traduction libre] (Europol, 2024, p. 14).

Le développement des technologies de machine learning s'est accéléré au début des années 2010 avec l'essor du deep learning (apprentissage profond). Ce dernier est fondé sur des réseaux de neurones artificiels, inspirés du fonctionnement du cerveau humain, permettant aux machines d'identifier des corrélations complexes dans d'importants volumes de données et d'améliorer leurs performances au fil du temps (Georges, 2019 ; Lacroux & Martin-Lacroux, 2021). Le deep learning est aujourd'hui mobilisé dans de nombreuses applications telles que la reconnaissance vocale, la reconnaissance d'images ou encore l'analyse de scènes vidéo.

Le machine learning, le deep learning ainsi que leurs algorithmes de vision par ordinateur (computer vision), qui permettent d'analyser et d'interpréter des informations visuelles issues d'images ou de vidéos, constituent le socle du fonctionnement des caméras augmentées (Quadrature du Net, 2023).

2.2.2 Big data et qualité informationnelle

L'amélioration des performances de l'IA s'explique en grande partie par l'augmentation exponentielle des données numériques disponibles depuis les années 2000 (Lafrate, 2018). Les algorithmes actuels nécessitent des ensembles de données massifs pour être entrainés, testés et ajustés (Gesny, 2019). L'avènement du Big Data a ainsi permis l'émergence d'applications plus efficaces et plus précises, notamment en matière d'analyse automatisée d'images (Georges, 2019 ; Le Pollotec, 2018).

Toutefois, la dépendance à la donnée n'est pas neutre. La nature, la qualité et la structuration des données conditionnent directement les performances de l'algorithme (Lacroux & Martin-Lacroux, 2021). Comme le soulignent Barocas et Sebst (2016), les biais présents dans les données d'entrainement peuvent être reproduits, voire amplifiés, par les systèmes intelligents. Cet enjeu est particulièrement crucial dans le domaine de la sécurité, où les décisions algorithmiques peuvent influencer la manière dont les comportements sont détectés, signalés ou interprétés.

Lors de l'utilisation des caméras augmentées, les données traitées peuvent inclure des caractéristiques physiques, comportementales ou contextuelles, soulevant ainsi des enjeux juridiques importants, notamment au regard du RGPD (Goodman & Flaxman, 2017). La question de la gouvernance des données, leur licéité, leur finalité, leur minimisation ou leur exactitude, devient dès lors centrale lorsque ces technologies sont déployées par les autorités publiques.

2.3 Applications de l'IA dans la sécurité publique

L'intégration de l'IA dans le domaine de la sécurité publique s'inscrit dans un contexte caractérisé par la croissance exponentielle du volume de données disponibles, le développement d'algorithmes toujours plus performants et la nécessité de répondre à des enjeux sécuritaires de plus en plus complexes. L'IA constitue un outil permettant de transformer les pratiques policières, d'améliorer l'efficacité des opérations et de renforcer les capacités d'analyse (Laurier, 2024 ; Berckmans, 2024 ; Europol 2024).

2.3.1 IA et police : vers une transformation structurelle

Les technologies d'IA permettent d'automatiser un ensemble de tâches répétitives ou chronophages (Castets-Renard, 2019 ; Javed & Noman, 2012). Grâce à leur capacité à traiter des quantités massives d'informations en temps réel, les algorithmes facilitent le travail des autorités, leur permettant ainsi de se focaliser sur les tâches prioritaires (Europol, 2024). Dans les pratiques policières, l'IA est notamment mobilisée pour analyser les images en temps réel, identifier des situations ou des objets particuliers, détecter automatiquement des comportements inhabituels, repérer des schémas récurrents, assister les enquêtes via la recherche automatisée d'informations et optimiser la gestion opérationnelle de grands évènements (Parlement Européen, 2020 ; Mohamed Kane, 2024).

La littérature internationale utilise le terme « *algorithmic policing* » pour désigner l'ensemble des pratiques policières basées sur l'IA, que ce soit pour automatiser des tâches, assister la prise de décision ou orienter les interventions (Ferguson, 2017). Cette notion englobe donc la police prédictive (predictive policing), l'analyse algorithmique des risques, la surveillance automatisée et la reconnaissance biométrique.

Brayne (2021) montre que l'IA transforme les organisations policières en institutions « orientées données », modifiant leurs méthodes de travail, leur culture interne et les priorités opérationnelles. Lum

et Isaac (2016) démontrent que les modèles prédictifs qui reposent sur des données historiques peuvent avoir une influence sur la cartographie des risques et sur la répartition des ressources policières, reproduisant parfois les bais structurels présents dans les données d'entrainement. Ces enjeux sont également présents dans l'utilisation des caméras augmentées.

2.3.2 IA, prévention et sécurité publique

Grâce à sa capacité d'analyse d'importants volumes de données, l'IA peut rapidement extraire de ces derniers des informations exploitables et ainsi permettre d'anticiper des situations ou d'identifier des risques (détection de tendances dans l'activité criminelle, identification de corrélations entre différents types de données). L'IA peut également prévoir des besoins de ressources sur base des tendances passées (Europol, 2024). Elle pourrait donc constituer une aide à la prise de décisions, ce qui est particulièrement pertinent lors de situations où les ressources sont limitées et que le temps est compté comme dans le cas d'un enlèvement par exemple (Europol, 2024). D'autant que « l'incapacité à prendre des décisions judicieuses peut avoir un impact sociétal profond et des conséquences négatives sur les libertés et les droits des citoyens » [traduction libre] (Europol, 2024, p. 12). Comme l'explique Ford (2015), les machines surpassent les humains pour les tâches répétitives, massives ou standardisées, ce qui en fait des outils de surveillance et de tri particulièrement efficaces.

L'IA peut être mobilisée pour renforcer la prévention situationnelle, notamment à travers la détection précoce d'incidents, la surveillance automatisée de zones sensibles, la prévention d'actes terroristes, la gestion d'évènements de masse, l'identification de comportement suspects (Poullet, 2021 ; Australian Institute of Criminology, 2003). Dans le même sens, De keersmaecker & Debailleul (2016), expliquent que l'IA s'immisce dans les outils de surveillance permettant ainsi d'atteindre les objectifs de la prévention situationnelle en diminuant la criminalité grâce au façonnement de l'espace public. La fondation Carnegie pour la paix internationale a mis en évidence, dans une étude de 2019, que 75 pays sur 176 utilisent déjà un système d'IA à des fins de surveillance (Feldstein, 2019).

Cependant, ces systèmes ne sont pas exempts de limites et leur efficacité dépend étroitement de la qualité des données et du contexte dans lequel ils sont déployés. Berckmans (2024) et Bromberg et al. (2018) soulignent que, mal encadrées, ces technologies peuvent alimenter une perception de surveillance généralisée et fragiliser la confiance des citoyens envers les forces de l'ordre.

2.3.3 Human-in-the loop et nécessité d'adaptabilité

Bien que l'IA augmente les capacités opérationnelles des organisations policières, elle ne remplace pas l'expertise humaine. Farzaneh et Boyer (2021) rappellent qu'il est nécessaire que les agents soient en mesure d'interpréter correctement les alertes automatisées et de replacer les analyses algorithmiques dans leur contexte. En effet, les machines ne sont pas capables de gérer des situations sortant du cadre prédéfini. Toujours selon ces auteurs, une telle approche nécessite d'investir dans le développement de nouvelles compétences humaines, à travers des systèmes éducatifs qui doivent constamment s'ajuster aux progrès technologiques, tout en préparant les futurs travailleurs à faire preuve de flexibilité. Cette hybridation entre capacités humaines et automatisation constitue un enjeu central pour éviter une confiance aveugle dans les algorithmes et pour garantir une prise de décision équilibrée. Ces outils doivent être utilisés avec prudence, dans le respect des droits fondamentaux et intégrés dans des cadres institutionnels robustes pour prévenir des dérives potentielles (Europol, 2024). De plus, il convient de souligner que les systèmes d'IA ne peuvent fonctionner efficacement qu'à condition de s'appuyer sur une infrastructure adaptée et suffisamment développée. La mise en œuvre et l'exploitation de cette infrastructure implique des coûts importants ainsi que des compétences spécifiques. L'accès à ces technologies peut, par conséquent, s'avérer difficile pour les administrations de petites taille (Europol,

2024). Ces enjeux apparaissent de manière particulièrement visible dans l'intégration des caméras augmentées, examinées dans la section suivante.

2.4 Caméras et algorithmes

Selon le rapport de l'observatoire d'Europol (2024), les flux d'images numériques connaissent une augmentation significative, notamment en raison de la multiplication des caméras de vidéosurveillance et des appareils personnels. Cette évolution soulève la nécessité d'en assurer une exploitation efficace. Dans ce contexte, l'intelligence artificielle apparait comme un levier particulièrement pertinent. Les caméras dites augmentées désignent l'intégration de traitements algorithmiques automatisés dans les dispositifs caméras afin d'analyser en continu les flux enregistrés et de détecter des évènements ou des comportements particuliers. Cette technologie repose sur des méthodes d'apprentissage automatique, notamment le deep learning, permettant d'extraire, classifier ou interpréter des informations visuelles en temps réel. Notons toutefois que toutes les fonctionnalités dites « intelligentes » ne relèvent pas nécessairement de l'IA. Certaines reposent sur des règles explicites et des paramétrages plutôt que sur des modèles appris. Quoiqu'il en soit, ces dispositifs occupent une place centrale dans les débats contemporains relatifs à la sécurité publique puisqu'elle se situe à l'intersection de préoccupations opérationnelles, éthiques, juridiques et sociétales. Comme le souligne Campion (2020), les questionnements et les débats sur la police belge mobilisent une pluralité d'acteurs allant de la hiérarchie policière aux responsables politiques, en passant par les citoyens et les chercheurs universitaires.

2.4.1 Définition et distinction entre « caméras biométriques » et « caméras augmentées »

La Commission nationale de l'informatique et de libertés (CNIL, 2022) distingue deux catégories principales de dispositifs caméras reposant sur l'IA. Cette distinction repose sur deux critères à savoir la nature des données traitées (caractéristique physique, physiologique ou comportementale) et l'objectif du dispositif (identifier ou authentifier de manière unique une personne). Ainsi, sont considérées comme « caméras biométriques », celles qui traitent des données biométriques permettant l'identification unique d'une personne (ex : reconnaissance faciale). Ces systèmes mettent en relation un gabarit biométrique préexistant et une image captée pour authentifier ou identifier un individu. Ils répondent donc aux deux critères. Comme le précise le rapport d'Europol (2024), « La combinaison de la biométrie et de l'IA permet d'allier efficacité et précision, offrant ainsi des informations détaillées qui permettent d'identifier rapidement et efficacement les criminels tout en protégeant la vie privée des personnes non concernées » [traduction libre].

Les « caméras augmentées », quant à elles, analysent les images afin de détecter des objets, des comportements ou des situations, sans identifier une personne de manière unique. Ces caméras peuvent donc répondre à un seul critère ou aucun, comme une caméra qui classifie simplement les usagers de la route, mais elle ne répondra jamais aux deux critères. Les caméras augmentées correspondent donc au traitement algorithmique non biométrique, tandis que la reconnaissance faciale (FRT) relève d'un traitement biométrique. L'intégration des algorithmes se fait via des logiciels permettant ainsi « une analyse automatique, en temps réel et en continu, des images captées par la caméra » (CNIL, 2022, p. 2). Les termes de caméras augmentées correspondent donc aux termes de vidéosurveillance algorithmique (VSA) ou de caméras intelligentes utilisés par certains auteurs. La littérature parle également de vidéoprotection. Dans un but de clarté et d'usage non connoté, nous parlerons de caméras augmentées dans cette recherche. D'autant que la loi belge sur la fonction de police parle de caméra et non de vidéosurveillance et que cette recherche porte sur les perceptions policières.

2.4.2 Fonctionnement des caméras augmentées et intégration des dispositifs dans les pratiques policières

Les caméras augmentées permettent d'analyser des données provenant d'images de caméras afin d'identifier des schémas types ou des activités suspectes qui n'auraient peut-être pas été détectées par l'œil humain comme par exemple, la détection de dépôts sauvages (Laurier, 2024). Cela est notamment rendu possible grâce aux outils de classification d'images (Europol, 2024). Le réseau mobile permet d'envoyer des flux vidéos haute définiton à grande vitesse, rendant alors possible l'analyse en temps réel des vidéos par les algorithmes. De plus, les caméras intègrent aussi une fonction de résumé vidéo qui permet « de parcourir et d'enregistrer de grandes vidéos dans des vidéos plus petites, économisant ainsi du temps et de l'espace » (Javed & Noman, 2012, p. 23). Ce résumé peut se composer soit uniquement d'images, soit d'une vidéo plus courte basée uniquement sur les éléments jugés pertinents (Javed & Noman, 2012).

L'analyse en temps réel, permet d'ouvrir de nouvelles possibilités pour le contrôle des foules en fournissant des informations sur la circulation des participants ou le potentiel encombrement d'une zone. Cela tend à faciliter une planification proactive (Laurier, 2024 ; Europol, 2024). Par ailleurs, les logiciels peuvent également déclencher des alertes automatiques s'ils détectent des incidents ou bien des éléments considérés comme suspect lors de leur analyse du flux vidéo. Ces alertes permettent, notamment, de signaler des troubles à l'ordre public ou bien des risques potentiels pour la sécurité. Puis, les opérateurs sont libres, selon leur appréciation, de donner ou non des suites à ces alertes (Europol, 2024 ; Quadrature du Net, 2023). Cela permet aux décideurs de se concentrer sur l'analyse et la réaction aux informations sélectionnées en amont par ordre d'importance. Cette procédure contribue donc à un meilleur rendement de la surveillance (Javed & Noman, 2012) et peut également permettre de réduire le nombre d'opérateurs nécessaires (Lastrayoli, 2024). Effectivement, les flux vidéo des caméras surveillant les espaces publics peuvent être centralisés dans un espace dédié au visionnage en temps réel ainsi qu'à la relecture des enregistrements vidéo, conservés pour une durée déterminée. Les opérateurs peuvent ainsi analyser les images enregistrées et établir un signalement en cas d'infraction. (Centre De Supervision Urbaine (CSU), n.d.). Certains filtres peuvent aussi être appliqués aux caméras afin de faire de la recherche paramétrée selon des critères tels que la couleur vestimentaire, le genre présumé ou le type d'objet (Debailleul, 2023).

Au vu de l'évolution constante des menaces et de la croissance des villes, il parait nécessaire de veiller à une utilisation optimale des ressources des forces de l'ordre qui opèrent généralement avec des budgets et des effectifs limités. Ainsi, l'IA et les technologies qu'elle permet de développer semblent avoir un rôle à jouer dans la planification stratégique et la sécurité publique (Europol, 2024).

2.4.3 Exemple d'utilisation des caméras augmentées et de la reconnaissance faciale

C'est à l'occasion des Jeux olympiques de Paris 2024 que l'utilisation de caméras augmentées a été autorisée pour la première fois à titre expérimental, en France, par la loi du 19 mai 2023 afin de répondre à l'enjeu sécuritaire de ce type de rassemblement (Tallent, 2024). Comme l'explique Laure et Michaël Laref (2025), des évènements historiques tels que ceux du drame du Heysel ou des Jeux de Munich ont impliqué « un renforcement des conditions et modalités devant entourer la tenue » de manifestations sportives de grande ampleur (p.68). Les dispositifs ont notamment été déployés pour identifier des mouvements de foule, des intrusions dans des zones interdites, des objets abandonnés ou des risques de densité anormale de personnes (Ministère de l'Intérieur, 2025).

Selon Zatsepina et Ludvigsen (2025), les Jeux de Paris 2024 constituent une étape importante dans l'évolution des dispositifs de surveillance utilisés lors d'évènements sportifs. Les auteurs expliquent que les Jeux olympiques représentent historiquement des « spectacles sécuritaires » dans lesquels les mesures de sécurité doivent être tant efficaces que visibles. Ils considèrent les Jeux de Paris comme s'inscrivant dans une dynamique plus large de recours croissant aux technologies de surveillance dans les démocraties contemporaines. D'autant que ces dernières sont marquées par des contexte de lutte contre le terrorisme et les risques d'atteintes graves à la sécurité des personnes. Ferrari (2022) considère quant à lui que les Jeux ont servi de terrain d'expérimentation pour de nouvelles technologies sécuritaires destinées à être progressivement intégrées dans l'espace public. L'auteur met en exergue un processus de normalisation de la surveillance technologique à travers l'utilisation de caméras augmentées, de drones et d'outils d'analyse automatisés des comportements. Laure et Michaël Laref (2025) le rejoignent en estimant que les grands évènements sportifs favorisent l'acceptation de mesures sécuritaires exceptionnelles qui par la suite tendent à s'ancrer durablement dans les politiques publiques de sécurité. De plus, cette sécurisation mobilise, selon eux, une collaboration entre une multiplicité d'acteurs tels que les pouvoirs organisateurs, des préfets, des maires, des acteurs de la sécurité privée, la police et les fournisseurs des systèmes technologiques. Ces auteurs adoptent une position critique de la généralisation de la surveillance, en soulevant notamment des risques pour les libertés fondamentales.

Le rapport du comité d'évaluation de l'expérimentation publié par le Ministère de l'Intérieur souligne toutefois un contraste dans les résultats obtenus. Les systèmes de caméras augmentées auraient principalement présenté un intérêt pour la détection d'intrusions et la circulation des personnes mais moins pour la détection de mouvement de foule, de la densité d'individus, d'objets abandonnés, de départs de feu ou de personne au sol à la suite d'une chute. Effectivement, « l'intérêt opérationnel du dispositif n'est pas négligeable ». « Cependant, il demeure encore limité pour différentes raisons, qui tiennent au caractère insuffisamment mature de la technologie et/ou aux besoins encore limités des opérateurs d'un tel appui en l'état des effectifs déployés sur place » (2025, p. 69). Le rapport précise que les opérateurs humains restaient chargés de vérifier les alertes produites par les algorithmes. Néanmoins, plusieurs fonctionnalités n'ont pas pu être évaluées de manière suffisamment approfondie en conditions réelles. Des difficultés liées aux faux positifs et à la pertinence de certaines alertes ont aussi été mises en évidence. Toujours selon le rapport, les performances dépendent également de la qualité du calibrage réalisé au préalable et l'intérêt opérationnel varie selon le contexte d'utilisation, la durée de l'entrainement des caméras, de la présence policière, de la durée de l'expérimentation, du choix des zones à risque ainsi que de l'aptitude à mobiliser des effectifs pour traiter et exploiter les alertes (Ministère de l'Intérieur, 2025).

Notons que les technologies de reconnaissance faciale automatisée (AFR) n'ont pas été autorisées lors des jeux olympiques et paralympiques. Pour rappel, ces dernières « autorisent la détection des sentiments, la reconnaissance automatique des personnes ayant commis tel ou tel fait ou autorisés à tel ou tel accès » (Poullet, 2021, p. 22). La reconnaissance faciale automatisée désigne une technologie permettant d'identifier et de différencier les données biométriques humaines de manière automatique grâce à des algorithmes entrainés à extraire et à analyser certains traits du visage au départ d'images ou de vidéos afin de comparer ou de vérifier les identités (Gates, 2011 cité par Bargias et al., 2021 ; Europol, 2024). La reconnaissance faciale peut dès lors être appliquée pour aider les forces de l'ordre dans leur pratique. En effet, cette technologie permet à la police d'identifier, rapidement et efficacement, de manière unique les criminels dans les espaces publics et dans les foules (Bragias et al., 2021 ; Mohamed Kane, 2024). La reconnaissance faciale peut aussi permettre de localiser des personnes portées disparues (Mohamed Kane, 2024). Il est à noter que la technique consistant à utiliser des images faciales pour identifier des criminels est très ancienne. « Jusqu'au début des années 1960, la procédure était

principalement manuelle et reposait sur la perception individuelle et la capacité humaine à reconnaitre des visages familiers » [traduction libre] (Europol, 2024 p. 23).

La reconnaissance faciale est largement déployée aux États-Unis et des millions de personnes sont déjà reprises dans des bases de données. Elle peut se faire en temps réel ou à postériori. Par contre, cette technologie n'est pratiquement pas réglementée et fait débat quant aux risques pour le respect de la vie privée et des libertés civiles ainsi que pour la protection des données. De plus, les erreurs d'identification et les biais algorithmiques constituent de véritables préoccupations (Gravie et al., 2016 ; Europol 2024). Le site officiel de la police métropolitaine de Londres présente cette technologie, qui est utilisée en temps réel et en a postériori, comme destinée à améliorer la sécurité publique et l'efficacité policière. Le discours se veut rassurant en insistant sur le contrôle humain, l'encadrement juridique et l'absence de biais selon des tests scientifiques du National Physical Laboratory (Metropolitan Police Service, n.d.). De plus, la police métropolitaine publie ses registres des déploiements de la reconnaissance faciale dans une volonté de légitimation institutionnelle par la transparence. Celui de 2026 met notamment en avant une utilisation ciblée et ponctuelle de cette technologie, basée sur des listes de personnes recherchées et des paramètres algorithmiques ajustables. Toutefois, l'absence de données relatives aux biais, aux erreurs globales ou au nombre total de personnes scannées limite fortement l'évaluation critique de l'impact de ces dispositifs sur les droits fondamentaux (Metropolitan Police Service, 2026). Ces approches contrastées soulignent l'ambiguïté de l'usage policier de la reconnaissance faciale alimentant ainsi les débats publics relatifs à son déploiement dans les espaces publics et privés, ainsi qu'aux questions de transparence, de consentement et de respect du cadre légal (Fussey & Murray, 2019).

L'évolution rapide des technologies de reconnaissance faciale crée un décalage entre la recherche académique et leur mise en œuvre, les études étant souvent menées après le déploiement des systèmes (Bargias et al., 2021). Sur le plan commercial, ces technologies sont proposées aux forces de l'ordre depuis les années 1990 (Gates, 2011 cité par Bargias et al., 2021), renforçant l'intérêt pour leur potentiel dans les enquêtes criminelles. En l'espace de trois décénies, la reconnaissance faciale est devenue un outil couramment utilisé par les services de police, gagnant en complexité et nécessitant une adaptation constante du cadre académique (Bargias et al., 2021).

2.5 Limites et défis des technologies liées aux caméras associées aux algorithmes

Malgré les bénéfices escomptés, ces technologies montrent des limites (Gakoue & Gakoue, 2013). La surveillance pose de nouveaux défis, tant technologiques que sociétaux (Lastrayoli, 2024). Les algorithmes d'apprentissage automatique ou « machine learning » soulèvent des questions éthiques (Besse et al., 2018 ; Hadjadji, 2024). Ces dernières « concernent principalement les problèmes de confidentialité des données, d'entrave à la concurrence, de transparence ou explicabilité des décisions, de leurs risques de biais discriminatoires envers des individus ou groupes sensibles » (Besse et al., 2018, p. 10). La prise de décision automatique via un algorithme peut potentiellement impacter les droits et libertés des individus (Castets-Renard, 2019). Dans son rapport de 2024, le laboratoire d'innovation d'Europol insiste sur la nécessité d'une utilisation conforme et responsable des technologies d'IA par les forces de police afin d'en garantir un déploiement efficace et éthique.
En se basant sur une étude du Pew Research Center, Hirose (2017) affirme que plus de 60 % des américains considèrent qu'il est important de pouvoir se déplacer en public sans être constamment identifié. Cela constitue un élément essentiel des valeurs sociales. Il est nécessaire que les systèmes d'IA soient conçus dans le respect de ces principes. « Ce n'est qu'alors que l'IA pourra être utilisée de manière responsable dans la pratique policière, en préservant la confiance du public et la protection des droits individuels. » (Berckmans, 2024, p. 3). Avec le recours à l'intelligence artificielle, le politique ainsi que

les acteurs opérationnels disposent d'instruments dotés d'une grande puissance. C'est pourquoi il est important de pouvoir réguler et encadrer l'usage de ces derniers (Lastrayoli, 2024). Il est important également de ne pas occulter les problématiques structurelles résultant de la dépendance au secteur privé.

2.5.1 Risques de biais et discriminations

Les IA d'apprentissage automatique apprennent à partir de grandes quantités de données (Gesny, 2019) sélectionnées et décrites par des humains qui ont leurs propres biais. La société contient des inégalités, de l'exclusion et d'autres types de discriminations. Par conséquent, selon Barocas et Selbst (2016), il y en aura inévitablement dans les données d'entrainement. Les données peuvent donc involontairement mener à des résultats biaisés ou injustes car l'IA va capter ces biais et les restituer (Lastrayoli, 2024) pouvant ainsi contribuer à renforcer des formes de ségrégation et de discrimination sociale, raciale (Castets-Renard, 2019) ou sexiste sans qu'il soit aisé d'en comprendre l'origine et de résoudre le problème (Debailleul, 2023). Or, « le droit à la non-discrimination est profondément ancré dans le cadre normatif qui sous-tend l'UE » [traduction libre] (Goodman & Flaxman, 2017, p. 3). Les articles 10 et 11 de la Constitution belge garantissent également le principe d'égalité et de non-discrimination.

Outre ces biais sociétaux, il y a également un risque de biais de représentation. En effet, si les données d'entrainement ne représentent pas l'ensemble de la population, alors les groupes surreprésentés dans ces données pourraient être disproportionnellement ciblés par les systèmes d'IA (Europol, 2024). Par exemple, l'âge, le genre ou l'origine ethnique des individus présents dans les données d'apprentissage peuvent influencer et biaiser le fonctionnement de l'algorithme (Lastrayoli, 2024). De manière générale, les données qui permettent d'entrainer les algorithmes ne correspondent pas toujours à la réalité que ces derniers ont à traiter (Georges, 2019). En outre, il existe des disparités dans les pratiques de collecte et de stockage des données en fonction des juridictions. Cela peut influencer la fiabilité et l'intégrité des résultats produits par l'IA (Europol, 2024).

A titre d'exemple de biais, nous pouvons mentionner la recherche de Larson et al., (2016) basée sur le système d'algorithme de justice prédictive COMPAS. Ce dernier permet de prédire les risques de récidive et aide le personnel judiciaire lors de leur prise de décision durant une procédure criminelle. Toutefois, leur étude dénonce les risques de discrimination, notamment raciale, liés à ce type d'outil. Nous pouvons également citer les logiciels de police prédictive présents dans les modèles informatiques comme PredPol. Ils peuvent mener à un ciblage excessif des communautés vulnérables quand ils sont utilisés pour se focaliser sur les « délits nuisibles » qui ont lieu dans les zones pauvres (Mateen, 2018). Le défi majeur aujourd'hui consiste à identifier ces biais et à mettre en place des mécanismes pour corriger les systèmes, tout en optimisant l'efficacité des résultats (Castets-Renard, 2019). D'autant que les biais sont difficilement détectables une fois introduits dans l'IA car son fonctionnement est « opaque » et aucun système d'identification de biais n'existe à ce jour (Lastrayoli, 2024).

2.5.2 Manque de transparence dans les processus décisionnels algorithmiques

Plusieurs auteurs tirent l'alerte sur l'opacité du fonctionnement des algorithmes complexes d'IA, fonctionnement dit en « boite noire » (Pasquale, 2016 ; Europol, 2024) et plaident en faveur d'une plus grande transparence dans les processus décisionnels algorithmiques (Goodman & Flaxman, 2017). « Les modèles fréquemment utilisés sont effectivement construits sur des corrélations et inférences plutôt que sur des causalités, ce qui rend impossible toute explication claire et compréhensible par l'Homme » (Castets-Renard, 2019, p. 4). « Tout comme une boite noire opaque et scellée, ces algorithmes produisent des résultats sans dévoiler leur fonctionnement interne, ce qui empêche d'évaluer la logique appliquée » [traduction libre] (Europol, 2024 p. 35). De plus, les algorithmes d'IA peuvent manquer de transparence en raison de leur protection au titre du secret des affaires (Europol, 2024). Or, il est légitime

de comprendre le fonctionnement des algorithmes afin de s'assurer de la validité de leurs calculs et de pouvoir en débattre publiquement (Cadron, 2018).
Les travaux existants soulignent la nécessité d'encadrer l'usage de ces technologies par des processus démocratiques transparents (Bargias et al., 2021). « La transparence dans la prise de décision en matière d'IA est essentielle pour garantir la responsabilité et la confiance » [traduction libre] (Klarin, 2024, p. 5). Dès lors, il indispensable que les agents de police, tout comme les personnes concernées par ces décisions, puissent comprendre le raisonnement qui les sous-tend. En l'absence de transparence, les risques de méfiance, d'abus et d'injustices potentielles sont susceptibles d'augmenter (Europol, 2024). Par ailleurs, le recours à l'intelligence artificielle par les forces de l'ordre soulève des enjeux sociétaux significatifs et fait l'objet de débats tant publics que politiques. Dès lors, il parait essentiel de favoriser la confiance et l'adhésion du public à l'égard de ces dispositifs (Europol, 2024).

2.5.3 Atteintes potentielles aux libertés et droits fondamentaux : responsabilité, transparence et explicabilité comme gage de confiance

La littérature indique que le public se montre souvent sceptique vis-à-vis de l'utilisation des nouvelles technologies par les forces de police (Bromberg et al., 2018). Il doit avoir confiance dans la façon dont la police utilise ces nouvelles technologies (dont celles de reconnaissance faciale) pour maintenir des relations solides entre la police et les citoyens. Cependant, les recherches ont illustré la possibilité pour ces nouveaux dispositifs d'altérer les relations entre la police et les citoyens s'ils ne sont pas légitimés notamment grâce à un processus démocratique avec un code de conduite clair pour leur utilisation (Bragias et al., 2021). Dans leur étude, Bradford et al. (2020) ont constaté que le public exprimait des préoccupations spécifiques à l'égard de l'utilisation des nouvelles technologies par les forces de police, telles que la crainte d'une atteinte à la vie privée, une mise en œuvre des technologies de manière non démocratique et un manque de confiance. Trouver un équilibre entre la sécurité publique et le respect de la vie privée constitue depuis longtemps un enjeu majeur. Avec l'intégration croissante de l'IA dans les pratiques policières, cet équilibre devient encore plus complexe à atteindre (Europol, 2024). L'étude de Bargias et al. (2021), relative à l'utilisation des technologies de reconnaissance faciale par la police, s'est également concentrée sur les préoccupations du public et en a dégagé trois principales. La première est liée à la précision de la technologie, la seconde se rapporte à la crainte des abus d'autorité et de pouvoir et la troisième se réfère à l'exploitation ou la suppression de leurs droits ou de leurs libertés. Selon le rapport du laboratoire d'innovation d'Europol (2024), il est essentiel de bénéficier de systèmes techniquement fiables mais également conformes aux principes d'équité et de justice. A cet égard, des exigences telles que la responsabilité, la transparence et l'explicabilité apparaissent fondamentales. Elles contribuent notamment à garantir que les preuves issues de systèmes d'IA puissent faire l'objet d'un examen rigoureux, respectant ainsi le droit à un procès équitable et soient reconnues comme recevables dans le cadre des procédures judiciaires. Le rapport insiste également sur la nécessité d'audits réguliers des systèmes d'IA afin de maintenir l'équilibre entre l'exploitation des informations fournies par l'IA et le respect des droits fondamentaux et libertés individuelles. D'autant que l'IA est une matière en perpétuelle évolution. Pour déployer l'IA dans le respect des principes d'équité, d'inclusion et de justice, tout en renforçant la confiance, il est recommandé aux services de police d'impliquer de manière proactive les différentes communautés afin d'avoir des points de vue allant au-delà d'une évaluation technique (Europol, 2024).
Il est à noter que dans certaines situations, le public peut soutenir l'utilisation des technologies d'IA. Par exemple, l'utilisation de la reconnaissance faciale a été soutenue pour identifier les émeutiers du Capitole (Lyons, 2021 cité par Bargias et al., 2021). Bargias et al. (2021), montrent, dans leur étude, que le public exprime un soutien envers cette technologie en ce qu'elle permet de maintenir l'ordre public. La plupart de leurs participants ont exprimé le désir de se sentir plus en sécurité. Toujours dans le cas de la reconnaissance faciale, bien que des lignes gouvernementales claires peuvent être définies, des

lacunes législatives ou des compromis entre sécurité publique, sécurité nationale et droits des citoyens peuvent créer des zones d'ombre. Par exemple quant aux lieux, aux moments et aux contextes d'utilisation. De plus, comme mentionné supra, les limites technologiques influencent aussi la façon dont cette technologie est déployée (Bargias et al., 2021).

Durant l'année 2016, la SNCF a testé des caméras intelligentes dans un but de détection des agressions mais les résultats n'ont pas été communiqués. En 2017, la reconnaissance faciale a été expérimentée lors du carnaval de Notting Hill mais elle n'a pas abouti en raison de nombreux « faux positifs » (Tallent, 2024). Lunter (2020) a évalué le logiciel de reconnaissance faciale FRT et a observé un taux de faux positifs plus élévé chez les personnes originaires d'Afrique de l'Ouest et de l'Est et d'Asie de l'Est comparé à celles d'Europe de l'Est.

2.5.4 Défis technique liés à l'intégration des outils d'IA

L'intégration de l'IA dans les systèmes des forces de l'ordre pose plusieurs défis techniques majeurs. Premièrement, l'incompatibilité entre les technologies récentes d'IA et les infrastructures existantes complique leur mise en œuvre ainsi que leur efficacité et nécessite une modernisation des systèmes actuels comme par exemple un renouvellement du parc caméra. Deuxièmement, ces technologies doivent rester performantes face à des volumes de données variables et à des contextes opérationnels complexes. Il est donc important de concevoir des modèles évolutifs et adaptables (Europol, 2024).

Par ailleurs, les systèmes d'IA requièrent des mises à jour, une maintenance continue et un support technique important. Cela peut représenter une contrainte pour les services de police disposant de ressources limitées. La mise en place de structures de soutien dédiées et de partenariats avec des acteurs technologiques apparait dès lors comme une solution pertinente. Toutefois, il est à noter que la commercialisation des nouvelles technologies tend à complexifier le processus (Mann & Smith, 2017 cité par Bargias et al., 2021). Ces technologies reposent souvent sur des services fournis par des entreprises privées car ces dernières disposent des infrastructures et des ressources nécessaires pour supporter ces systèmes coûteux. En effet, « le développement et le déploiement efficaces des technologies d'intelligence artificielle nécessitent une infrastructure technologique et un savoir-faire considérable, ce qui pose des défis de taille, en particulier aux services de police de petite taille » [traduction libre] (Europol, 2024, p. 10). Ces technologies peuvent donc effectuer une transition de bien public à bien privé. Ce passage tend à limiter l'influence du gouvernement et des forces de l'ordre sur le déploiement de ces technologies (Mann & Smith, 2017 cité par Bargias et al., 2021). De surcroit, ces entreprises privilégient généralement une autorégulation du marché plutôt qu'un encadrement législatif strict, contraignant la police à collaborer avec ces acteurs privés (Introna & Nissenbaum, 2010).

S'agissant de la consultation des images de caméras par des acteurs privés, le gouvernement fédéral dirigé par Bart De Wever manifeste une volonté de l'encourager. En effet, cela est considéré comme un soutien aux services de police. L'intention est de modifier la législation afin « d'établir une distinction claire entre l'utilisation policière et non policière des caméras. Dans ce dernier cas, la police est considérée comme le responsable du traitement et de la visualisation en temps réel des images de la caméra qui ne peut se faire que dans les locaux de la police et sous la supervision d'un fonctionnaire de police présent » (Belgium.be, 2025 p. 141-142).

2.6 Cadre juridique relatif à l'utilisation des caméras par les services de police

L'encadrement juridique de l'utilisation des caméras repose sur un ensemble de dispositifs européens et nationaux visant à protéger les droits fondamentaux tout en permettant aux autorités policières d'assurer la sécurité publique. Dans ce cadre, seules les dispositions les plus pertinentes pour cette recherche seront présentées.

2.6.1 Loi du 21 mars 2007 réglant l'installation et l'utilisation des caméras de surveillance (2007, modifiée en 2018) – Législation nationale belge

La loi dite « caméra » encadre l'installation et l'usage des caméras. Elle impose des obligations de signalisation, des conditions strictes de proportionnalité, des règles de conservation et d'accès aux images ainsi que les finalités autorisées (prévention d'infractions, maintien de l'ordre public, sécurité des biens et des personnes). Cette loi s'applique aux caméras fixes et mobiles. Elle distingue trois types de lieux, ouverts, fermés accessibles au public et fermés non accessibles au public.

2.6.2 Loi du 5 août 1992 sur la fonction de police (LFP) - Législation nationale belge

Cette législation constitue la base juridique spécifique pour la fonction de police. Elle a été modifiée à plusieurs reprises afin d'intégrer notamment certaines dispositions relatives à l'utilisation des caméras et des technologies de surveillance. En effet, loi du 21 mars 2018 a permis l'insertion des articles 25/1 à 25/8 réglant ainsi l'utilisation des caméras par les services de police. Les articles 25/2 à 25/5 autorisent les services de police à utiliser différentes catégories de caméras dans l'exercice de leurs missions. On distingue les caméras fixes, fixes temporaires, mobiles ainsi que les caméras intelligentes. Ces dernières sont autorisées uniquement si elles ne sont pas reliées à des fichiers de données à caractère personnel. Il existe une exception à l'article 26 pour l'utilisation des caméras « ANPR », dotées d'une capacité de reconnaissance automatique des plaques d'immatriculation des véhicules. La loi du 22 mai 2019 a modifié diverses dispositions de la LFP en ce qui concerne la gestion de l'information policière afin de préciser notamment les registres à tenir ainsi que les obligations de documentation interne lors de l'utilisation des caméras. La loi sur la fonction de police a à nouveau été modifiée par la loi du 19 octobre 2023 afin d'insérer de nouveaux articles relatifs à l'utilisation des caméras individuelles (bodycams) par les services de police.

2.6.3 Loi du 30 juillet 2018 sur la protection des personnes physiques à l'égard du traitement des données – Législation nationale belge

Cette loi transpose le RGPD et la directive police (UE 2016/680) en droit belge. Elle encadre le traitement des images, l'accès aux données, la durée de conservation ainsi que les droits des personnes filmées. La vidéosurveillance implique le traitement de données à caractère personnel. Par conséquent, elle impose le respect des règles de protection des données.

2.6.4 Le Règlement général sur la protection des données (RGPD) – Législation européenne

Le RGPD (2016) constitue le principal instrument juridique européen encadrant le traitement des données à caractère personnel. Ce Règlement est transposé en droit belge par la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. Une donnée est dite à caractère personnel lorsqu'il s'agit d'une information « se rapportant à une personne physique identifiée ou identifiable » (art. 4, 1). Les données sensibles sont des données à caractère personnel telles que des données génétiques, biométriques ou relatives à des convictions religieuses, qui ne peuvent, en principe, pas être traitées (art. 9).

2.6.5 La directive (UE) 2016/680 du 27 avril 2016 – Législation européenne

La Directive (UE) 2016/680, adoptée en parallèle du RGPD, encadre le traitement des données personnelles par les autorités compétentes à des fins de prévention, détection ou poursuite des infractions. Elle complète en imposant notamment un traitement nécessaire et proportionné, une finalité strictement sécuritaire, des obligations renforcées d'exactitude, de sécurité et de minimisation.

Les forces de l'ordre évoluent dans un cadre juridique et éthique complexe qui exige une adaptation constante afin de garantir des pratiques de gestion des données à la fois responsables et efficaces (Europol, 2024).

2.7 Cadre juridique relatif à l'utilisation de caméras augmentées

Actuellement, il n'existe aucune réglementation nationale belge qui encadre l'utilisation d'une telle technologie. En revanche, au niveau européen, une première réglementation a été établie en matière d'intelligence artificielle.

2.7.1 Le Règlement européen sur l'intelligence artificielle 2024 (IA Act) : un cadre européen fondé sur les risques – Législation européenne

Publiée au Journal officiel de l'Union européenne (UE) le 12 juillet 2024, cette nouvelle législation européenne introduit un ensemble de normes et de lignes directrices qui devront être prise en compte lors de l'utilisation de système d'IA au sein de l'Union européenne. Cette législation vise à concilier la protection des valeurs fondamentales de l'UE avec l'intégration de technologies d'IA dans les pratiques des forces de l'ordre. Les services répressifs devront, dès lors, veiller à ce que leurs outils d'IA actuels et futurs soient conformes à la législation (Europol, 2024). C'est une approche basée sur le risque qui a été adoptée. Plus les applications d'IA présentent des risques, plus les règles les concernant seront strictes. Certaines pratiques y sont même interdites telles que la police prédictive basée sur le profilage et la classification à l'aide de données biométriques par catégorie comme la race, la religion et l'orientation sexuelle. Les obligations de transparence sur les données utilisées ont été renforcées (*BOSA*, s. d.).

L'AI Act interdit aussi les systèmes d'identification biométrique en temps réel et à distance comme la reconnaissance faciale. Toutefois, dans certains cas elle peut être exceptionnellement autorisée par exemple si son utilisation est strictement nécessaire « pour la recherche ciblée de victimes potentielles spécifiques de la criminalité, notamment d'enfants disparus (art. 5 §1, d), i) IA Act) » ou en prévention d'une attaque terroriste (art. 5 §1, d), ii IA Act). L'AI Act sera applicable deux ans après son entrée en vigueur, sauf exceptions. Cependant, les dispositions relatives aux pratiques interdites sont applicables depuis début février 2025 (*BOSA*, s. d.).
Puisque la législation européenne sur l'IA est appelée à influencer le développement des futurs systèmes, une collaboration entre les forces de l'ordre, les chercheurs en IA, les développeurs ainsi que les experts en éthique et en protection des données semble indispensable. Dans cette perspective, de nouveaux dispositifs tels que les « regulatory sandbox » ainsi que des « data spaces » peuvent constituer des mécanismes d'adaptation pertinents surtout lorsque l'usage des technologies basées sur l'IA est susceptible de porter atteinte aux droits et libertés des citoyens. Le but de ces dispositifs est d'offrir des environnements contrôlés dans lesquels ces outils peuvent être testés et ajustés sans impact direct sur le monde réel. Ainsi, les services répressifs s'assurent que les systèmes répondent à la fois aux exigences opérationnelles et juridiques avant que ces derniers ne soient déployés. Cette approche favorise des ajustements continus tout en contribuant à instaurer un cadre propice à l'innovation (Europol, 2024).

Concernant l'utilisation de caméras augmentées, il est également nécessaire de se conformer aux prescrits du RGPD. En effet, elles peuvent analyser les émotions et les comportements, impliquant le traitement de données à caractère personnel. Ces informations peuvent également être considérées comme sensibles, nécessitant dès lors une protection renforcée en raison de leur impact sur les libertés individuelles et les droits fondamentaux (considérant 51 RGPD). Les responsables du traitement doivent donc être attentifs à la licéité du traitement (RGPD, 2016, art. 6), la finalité du traitement (RGPD, 2016, art. 5, §1, b), la minimisation des données (RGPD, 2016, art. 5, §1, c), la qualité ainsi que l'exactitude des données (RGPD, 2016, art. 5, §1, d). Ils doivent également veiller à la conservation limitée des

données (RGPD, 2016, art. 5, §1, e), l'obligation d'intégrité et de confidentialité (RGPD, 2016, art. 5, §1, f), la transparence (RGPD, 2016, art. 5, §1, a), le droit des personnes (par exemple, accès, information, rectification, etc) (RGPD, 2016, art. 13-22). Les responsables de traitement doivent aussi être attentifs à garantir une protection particulière aux données sensibles (RGPD, 2016, art. 9). Ils doivent veiller à la protection des données dès leur conception et à la protection des données par défaut (RGPD, 2016, art. 25).

L'article 22 du RGPD (2016) offre une protection supplémentaire en garantissant le droit de ne pas être soumis à une décision fondée exclusivement sur un traitement automatisé. Cette disposition met en avant la nécessité du contrôle humain dans le processus.

Notons qu'il convient d'être attentif à la hiérarchie des normes. Une norme inférieure ne peut pas contredire une norme supérieure. En cas de contradiction, la norme supérieure prime (Depussay, 2007).

Positionnement et intentions du gouvernement belge par rapport à l'intelligence artificielle

Au niveau national belge, un Comité Consultatif d'Éthique des Données et de l'Intelligence Artificielle de l'Administration Fédérale a été créé par l'Arrêté royal du 04 octobre 2023. Nous pouvons lire à l'article 4 que le Comité est compétent pour rendre des avis scientifiques sur plusieurs matières concernant l'intelligence artificielle, la robotique et les technologies connexes soit sur demande d'un service fédéral ou d'un membre du gouvernement fédéral, soit de sa propre initiative pour le compte d'un service fédéral ou d'un membre du gouvernement fédéral (Arrêté royal du 4 octobre 2023, art. 4). Le but de la création d'un tel Comité est de renforcer la confiance envers ces technologies et de veiller à ce qu'elles soient développées et utilisées dans le respect des exigences légales, éthiques et techniques.

Une proposition de loi a également été déposée le 17 décembre 2024 par Paul Van Tigchelt à la Chambre des Représentants (Chambre des représentants de Belgique, 2024). Cette proposition vise à insérer un nouvel article dans le Code d'instruction criminelle afin de permettre l'application en droit belge de l'article 5, paragraphe 5, du Règlement (UE) 2024/1689 sur l'intelligence artificielle. Actuellement, le texte est en cours d'examen parlementaire.

Dans l'accord de coalition fédéral du 31 janvier 2025, il est possible de percevoir une volonté de numérisation de la police intégrée afin de la rendre plus efficace, d'améliorer sa communication avec les citoyens et d'optimiser sa gestion interne tout en intégrant les technologies émergentes dans un cadre légal éthique et strict. A cette fin, il semble, au regard de cet accord, nécessaire que la police intégrée dispose d'outils informatiques (big data, détection des processus criminels dans le monde numérique etc.) (Belgique, 2025 p. 144-145). Le gouvernement fédéral préconise le développement « d'une stratégie de numérisation claire et à long terme pour la police » […]. Une stratégie numérique implique de revoir et d'optimiser les processus opérationnels selon les principes du digital-by-design et la protection de la vie privée » (Belgique, 2025 p. 145). Le gouvernement dirigé par Bart De Wever entend s'inscrire dans le cadre européen relatif à l'intelligence artificielle (IA Act) en développant des politiques concrètes encadrant le déploiement de ces technologies. Dans ce contexte, il est prévu de faciliter, dans un cadre juridique strictement défini, des champs d'expérimentation pour de nouvelles technologies, telles que la technologie de reconnaissance faciale pour la détection de condamnés ou de suspects. En outre, une extension de la législation relative aux caméras est envisagée afin de permettre un recours aux dispositifs de surveillance intelligente. (Belgique, 2025).

2.8 Contrôle des pratiques policières

En Belgique, le contrôle des pratiques policières relève de plusieurs niveaux et organes qui peuvent être juridictionnels, administratifs ou indépendants. Nous nous intéresserons à trois d'entre eux.

2.8.1 Autorité de protection des données (APD)

L'APD, organe de contrôle indépendant, joue un rôle crucial dans la protection des droits fondamentaux face aux technologies de surveillance en veillant au respect du RGPD et de la loi belge du 30 juillet 2018. Elle est notamment compétente pour évaluer les traitements à hauts risque, contrôler les autorités publiques, formuler des avis, sanctionner des violations (Autorité de protection des données, n.d.).

L'APD s'inscrit dans une démarche visant à promouvoir le développement d'une intelligence artificielle à la fois innovante et respectueuse des données personnelles. A ce titre, elle figure parmi les vingt autorités de protection des données ayant signé une déclaration conjointe intitulée « Join Statement on Trustworthy Data Governance for AI ». Cette déclaration plaide en faveur de la mise en place d'un cadre de gouvernance des données fiable, destiné à garantir le développement d'une intelligence artificielle digne de confiance. Bien que la déclaration mette en avant les opportunités offertes par ces technologies, elle souligne les risques significatifs qu'elles comportent notamment en matière de protection des données personnelles, mais aussi de discrimination et de désinformation, souvent liés à un traitement inadéquat des données. Les autorités signataires insistent sur la nécessité d'une gouvernance des données robuste ainsi que sur l'intégration des principes de protection des données dès la conception (privacy by design) (Autorité de protection des données, 2025 ; CNIL, 2025).

2.8.2 Organe de contrôle de l'information policière (COC)

Le COC constitue une garantie institutionnelle essentielle, complémentaire à l'APD, pour encadrer les pratiques policières. « L'Organe de contrôle est l'institution parlementaire fédérale autonome en charge de la surveillance de la gestion de l'information policière, et est l'autorité de protection des données pour la police intégrée, l'unité d'information des passagers et l'inspection générale de la police fédérale et de la police locale » (Organe de contrôle de l'information policière, *n.d.*, section Home). Le COC a joué un rôle clé dans plusieurs dossiers récents comme les tests de reconnaissance faciale à l'aéroport de Zaventem en 2017 et en 2019 ainsi que l'utilisation du logiciel Clearview AI (Démocratie.brussels, *n.d.*).

2.8.3 Le comité permanent de contrôle des services de police (Comité P)

« Le Comité P entend contribuer au bon fonctionnement d'une police démocratique, intègre et de proximité » (Comité P, n.d.). Il constitue l'institution externe encadrée par le parlement fédéral chargée du contrôle du fonctionnement global des services de police, d'inspection ou de contrôle ainsi que de la surveillance de la correcte exécution de la fonction de police par l'intégralité des fonctionnaires compétents. Le comité P veille notamment à l'efficacité, l'efficience et la coordination des services mais aussi au respect et à la promotion des libertés et droits fondamentaux.

En tant qu'observatoire de la fonction de police, le Comité P, sur base de ses enquêtes et analyses, d'initiative ou sur demande, tend à actualiser en permanence l'image globale de la police, examiner et évaluer le fonctionnement des services et formuler des propositions et avis aux autorités de police compétentes.
Par ailleurs, certains enquêteurs spécialisés sont affectés aux enquêtes judiciaires menées pour les besoins des autorités judiciaires. Ces enquêtes concernent prioritairement les domaines sensibles tels que les atteintes aux droits fondamentaux, les abus de pouvoir ou les dysfonctionnement graves dans l'exercice des missions policières.

Dans ce cadre, le Comité P peut être amené à examiner l'utilisation des technologies relatives aux caméras afin d'en vérifier la conformité aux normes légales et aux principes de proportionnalité et de légitimité (Comité P, n.d.).

2.9 État des lieux des dispositifs caméras en Belgique

L'usage des caméras s'est intensifié, en Belgique, au cours des deux dernières décennies, porté par les enjeux de sécurité publique, la lutte contre le terrorisme, la gestion de l'espace urbain et les politiques locales de prévention. L'introduction progressive d'outils tels que les caméras augmentées s'inscrit dans ce mouvement. Cette section expose les principales tendances observées en Belgique.

2.9.1 Une expansion continue des caméras : du réseau classique à la vidéo intelligente

L'utilisation des caméras est en augmentation au cours de la dernière décennie (Javed & Noman, 2012). La Belgique ne déroge pas à cette pratique. En 2014, le CRIB (Centre d'informatique pour la Région bruxelloise) donne 4 objectifs afin de faire de Bruxelles une « Smart City » c'est-à-dire, une région connectée, durable, ouverte et sécurisante (Bocquet, 2021). Parmi les objectifs, on retrouve « la mutualisation de la vidéoprotection » qui s'impose rapidement comme le chantier principal en raison d'un contexte politique favorable (Bocquet, 2021). Le réseau de caméras s'est considérablement élargi à Bruxelles au cours de ces dernières années pour lutter contre l'insécurité et le terrorisme, contre des dépôts clandestins et pour réguler le trafic des zone de basses émissions (Debailleul, 2023). Des évènements tels que les attentats viennent plaider pour l'installation de caméras plus performantes. Les caméras ANPR, capables de lire les plaques d'immatriculation, se déploient également (Debailleul, 2023).

De nombreuses institutions étatiques disposent de caméras sur la voie publique, ce qui engendre un problème de coordination pour la police (Bocquet, 2021). Debailleul (2023), nous apprend que les images de ces caméras partent en destination du dispatching de chaque zone de police mais aussi en direction de « Safe.brussels » qui a des missions de coordination des actions des acteurs de la sécurité publique (Lastrayoli, 2024). Ces caméras facilitent le quotidien de la police.

2.9.2 Un déploiement territorial inégal et corrélé à des facteurs socioéconomiques

Le déploiement des caméras n'est pas uniforme (De Keersmaecker & Debailleul, 2016). Par exemple, plus on s'éloigne du centre de Bruxelles moins il y en a (Debailleul, 2023). De plus, « Cette diminution se fait néanmoins de manière très inégale : en allant vers les quartiers plus aisés du sud-est (Boitsfort, Auderghem, Woluwé, etc.) on trouve beaucoup moins de caméras que si on se dirige vers le nord-ouest, et notamment vers les quartiers populaires jouxtant le canal comme Cureghem ou Molenbeek, qui sont, eux, particulièrement vidéosurveillés » (Debailleul, 2023, p. 12). Matongé, quartier congolais historique abritant une population pauvre et connaissant des problèmes de drogues, a été l'un des premiers endroits équipés et l'un des plus surveillés lorsque des caméras ont été installées dans la zone de police de Bruxelles Capitale Ixelles (De Keersmaecker & Debailleul, 2016). L'importance des facteurs socioéconomiques a été confirmée par une analyse quantitative (De Keersmaecker & Debailleul, 2016).

2.9.3 Introduction progressive de la vidéo intelligente : l'exemple de BriefCam

Plusieurs zones de police belge ont recours à des logiciels de résumé vidéo tels que Briefcam, notamment utilisé à Bruxelles. Il fournit un « résumé » puis effectue un tri des événements selon un critère de recherche tel que la couleur des vêtements ou le genre d'une personne suspectée (Debailleul, 2023) permettant ainsi un gain de temps et d'espace. Ce logiciel est basé sur sa technologie brevetée Video Synopsis (VS) (Javed & Noman, 2012).

Le logiciel inclut une fonctionnalité de reconnaissance faciale, actuellement proscrite par le cadre légal sauf exception (Debailleul, 2023). Ces données incluent les données biométriques permettant de détecter un individu par une IA (Lastrayoli, 2024). Certains projets locaux européens « contournent » la barrière du consentement. C'est-à-dire qu'ils se basent plutôt sur « la reconnaissance d'éléments corporels » tels que l'âge, les vêtements, le genre, les cheveux ou la forme du corps. La loi ne considère pas ces données, lorsqu'elles sont prises individuellement, comme biométriques (Lastrayoli, 2024). Toutefois, comme mentionné supra, l'IA Act permet l'utilisation de la reconnaissance faciale par les forces de l'ordre, sous conditions, dans trois exceptions.

2.9.4 Débats actuels et projets controversés en Belgique

En 2023, le Parlement bruxellois a reçu une pétition en faveur de l'interdiction de la reconnaissance faciale à Bruxelles (Démocratie.brussels, n.d.) témoignant d'une inquiétude publique accrue quant à l'usage des outils biométriques.

Au-delà de Bruxelles, plusieurs autres projets sont controversés au niveau national comme les tests des caméras intelligentes anti-GSM qui ont été interrompus puisque le COC a signalé que ces tests étaient non conformes à la législation (Info, 2022).

Trouver un équilibre entre sécurité et acceptabilité sociale est un défi majeur. Alors que le crime organisé adopte des technologies avancées, la police se retrouve dans une position délicate. Elle doit concilier lutte contre la criminalité à l'aide d'outils modernes et maintien de sa légitimité auprès du public (Bargias et al., 2021).

L'état des lieux de la littérature démontre que la Belgique se trouve dans une phase de transition. Les caméras « classiques » sont largement implantées, les caméras « augmentées » émergent progressivement mais manquent de cadre juridique clair. Les usages restent fragmentés et dépendent des initiatives locales. Le coût de ces technologies peut également freiner leur implantation, alors que la pression politique encourage quant à elle l'innovation. Peu d'études portent spécifiquement sur l'intégration des caméras augmentées en Belgique. Leurs effets différenciés selon les contextes socioéconomiques sont encore peu explorés. Les pratiques concrètes des policiers locaux face à ces technologies sont également peu documentées. Cela justifie, par conséquent, la pertinence d'une recherche centrée sur cette thématique. Ainsi, nous tenterons, dès lors, au travers de notre recherche de répondre à la question suivante : « Comment les fonctionnaires dirigeants des zones de police locale belges perçoivent-ils l'intégration des technologies algorithmiques associées aux systèmes de caméras dans les pratiques policières liées au maintien de l'ordre public au sens large, ainsi que leurs impacts potentiels sur la sécurité publique et les droits fondamentaux ? ».

3. Méthodologie

3.1 Type de recherche

Notre étude s'inscrit dans une démarche qualitative car elle vise à comprendre en profondeur les perceptions, raisonnements et expériences des fonctionnaires de police locale face à l'utilisation, encore expérimentale, des caméras augmentées en Belgique. Étant donné que le cadre juridique national n'en permet pas encore un déploiement généralisé, seules certaines zones de police ont mené des tests limités. Cette situation implique que les usages, les pratiques et les discours varient fortement d'une zone à l'autre. Afin de saisir cette diversité, nous avons opté pour un design multi sites, incluant plusieurs zones de police de tailles différentes, présentant divers degrés de maturité technologique et des partenariats distincts. Cette stratégie permet également d'observer des configurations variées (zones urbaines denses, zones mixtes, zones provinciales). Des entretiens ont ainsi été réalisés auprès de fonctionnaires

travaillant au sein de zones de type 1, 2, 3, 4 et 5 selon la typologie officielle des zones de police (Police fédérale, 2011).

Le caractère qualitatif de notre démarche est soutenu par les fondements méthodologiques décrits par Paillé et Mucchielli (2021). Nous avons conçu une méthode et des instruments dans le but de recueillir des données qualitatives à savoir des témoignages. Nous avons privilégié l'analyse du sens plutôt que la quantification puisque notre volonté est d'extraire le sens des propos plutôt que de les transformer en pourcentages ou en statistiques. La recherche peut également être qualifiée de qualitative dans le sens où « l'ensemble du processus est mené d'une manière « naturelle », sans appareils sophistiqués ou mises en situation artificielles, selon une logique proche des personnes, de leurs actions et de leurs témoignages » (Paillé & Mucchielli, 2021, p. 15). Pour ces auteurs, la méthode qualitative permet de « mettre à profit les capacités naturelles de l'esprit du chercheur et vise la compréhension et l'interprétation des pratiques et des expériences plutôt que la mesure de variables à l'aide de procédés mathématiques » (Paillé & Mucchielli, 2021, p. 15). Cet argument transparait également dans les propos de Bouchard et Cyr (2005), pour qui la méthodologie qualitative est préférable lorsqu'il s'agit d'essayer de comprendre les pratiques professionnelles.

Pour analyser nos données, nous avons opté pour l'analyse thématique telle que conceptualisée par Paillé et Mucchielli (2021) qui a pour but d'établir une vision globale d'un corpus théorique par le biais de thèmes. Toutefois, ces auteurs précisent que le chercheur ne thématise pas dans le but de résumer le texte mais plutôt dans le but de l'analyser. En effet, l'analyse thématique a pour fonctions principales une fonction de repérage et une fonction de documentation. L'objectif de notre recherche étant de comprendre les conséquences, avantages et limites des caméras augmentées du point de vue des fonctionnaires de police au niveau local, nous ne partons pas d'hypothèses fermes. La volonté d'exploration nécessite une méthode qui laisse émerger les thèmes directement à partir des discours. De plus, nous interrogeons différents profils avec des expériences variées (DPO, référents techniques, cadres). L'analyse thématique nous permettra dès lors d'identifier des convergences et divergences à travers un corpus hétérogène. Cette méthode d'analyse est également flexible, accessible et transparente car elle suit des étapes claires (Paillé & Mucchielli, 2021).

Dans cette recherche, nous ne voulons pas simplement décrire l'intégration des caméras augmentées, nous interrogeons aussi leurs impacts sociaux, juridiques et organisationnels. Étant donné que nous cherchons à comprendre comment les fonctionnaires de police vivent et interprètent cette intégration, les thèmes ne sont pas connus à l'avance mais émergent dans les interactions entre les données et notre analyse. Par conséquent, l'analyse thématique a été choisie sous sa forme réflexive telle que proposée par Braun et Clarke (2006, 2019). Ils proposent une analyse en six étapes qui seront respectées (familiarisation avec les données, génération de codes initiaux, recherche de thèmes, révision des thèmes, définition et dénomination des thèmes, rédaction du rapport analytique). Cette approche correspond mieux aux objectifs exploratoires de la recherche.

3.2 Échantillon et stratégie d'échantillonnage

La population ciblée dans notre recherche correspond aux fonctionnaires dirigeants des zones de police locales belges ayant une expérience, directe ou indirecte, dans l'utilisation de caméras classiques et/ou impliqués dans des réflexions relatives aux caméras augmentées. En raison des limites techniques de notre recherche, nous avons fait le choix de cibler certaines zones locales tout en veillant à une logique de variation. Nous avons sélectionné à la fois des grandes agglomérations marquées par une forte densité urbaine et des enjeux sécuritaires élevés, des zones semi-urbaines ainsi que des zones semi-rurales, où les réalités organisationnelles et les ressources disponibles diffèrent. Par cette sélection, nous avons tenté d'introduire une diversité contextuelle et socio-économique dans l'échantillon. Cela nous permet de favoriser la comparaison des pratiques et des perceptions liées à l'intégration des caméras augmentées grâce à des environnements contrastés.

Nous avons retenu une stratégie d'échantillonnage raisonné non probabiliste, reposant sur une diversification interne des profils au sein d'un groupe homogène de fonctionnaires dirigeants des zones de police locales belges (Savoie-Zajc, 2007 ; Paillé & Mucchielli, 2021 ; André, 2023). Les participants ont été sélectionnés en fonction de leur rôle, de leur expertise et de leur implication dans l'usage des caméras, le cas échéant algorithmiques. Pour garantir cette diversité au sein de notre échantillon, nous avons tenté d'inclure différents profils dirigeants tels que des opérateurs du Poste de Commandement Opérationnel, des cadres ainsi que des référents techniques et des DPO (Délégué à la Protection des Données). En recherche qualitative, l'échantillon ne doit pas viser la représentativité statistique mais plutôt la richesse et la diversité des données. Cette diversification des fonctions interrogées nous a ainsi permis de comprendre l'impact de l'intégration des caméras augmentées à plusieurs niveaux : pratique, opérationnel, organisationnel et éthique.
Pour des raisons organisationnelles et professionnelles, la plupart des zones n'ont pu mobiliser qu'un seul participant. La charge de travail importante des fonctionnaires a limité leur disponibilité. De plus, au vu de ce critère, les zones de police nous ont généralement dirigé d'initiative vers des fonctionnaires dirigeants.
Pour pouvoir participer à la recherche, les critères d'inclusion étaient les suivants :

Critères d'inclusion

- Homme/Femme/Autre (H/F/X)
- Être fonctionnaire de police au sein d'une zone de police locale belge
- Le régime linguistique du participant (francophone ou bilingue français/néerlandais)
- Avoir un lien professionnel avec l'utilisation des caméras (opérationnel, technique, décisionnel ou juridique)

Afin d'accéder à notre échantillon, nous avons utilisé la stratégie d'échantillonnage boule de neige (ou snowball sampling) en complément des contacts institutionnels via les sites officiels des zones de police. L'échantillonnage boule de neige consiste à recruter des participants pour une étude en demandant à ceux déjà recrutés de recommander d'autres personnes qui correspondent aux critères de recherche (André, 2020-2021). Les agents de l'autorité publique sont soumis au secret professionnel et à une forte hiérarchie. Par conséquent, il est plus difficile d'atteindre les participants au moyen d'une simple annonce ou d'un appel public. En outre, aucune liste publique ne recense les fonctionnaires exposés à aux dispositifs caméras intégrant des algorithmes. Dès lors, le soutien d'un supérieur hiérarchique ou d'un collègue lors de la prise de contact avec un participant constitue une aide non négligeable.
Cette double stratégie a permis de constituer un échantillon diversifié malgré les contraintes institutionnelles, tout en respectant l'éthique et la confidentialité propres au contexte policier. Toutefois, il est à noter que la majorité des participants appartiennent aux tranches d'âge 26 – 35 ans (2) ; 36 – 45 ans (5) et 46 – 55 ans (6). Nous arrivons à un total de 13 car le participant 7 était accompagné lors de l'entretien. Un tableau récapitulatif des participants est présenté en annexe (Annexe 1).

3.3 Organisation de l'entretien

Les participants ont eu la possibilité de choisir une entrevue en présentiel ou en distanciel par le biais d'une visioconférence. Cinq entretiens ont été réalisés en présentiel, dans les locaux des zones concernées, tandis que les sept autres ont été réalisés en visioconférence. Cette flexibilité a permis de respecter la charge de travail des participants.

Les entretiens ont duré entre 1h et 2h40, selon l'expérience du participant, l'ampleur de ses responsabilités et son degré d'implication dans l'intégration potentielle de caméras augmentées. Un formulaire de consentement éclairé (Annexe 3) reprenant une description de l'étude, les considérations éthiques, la confidentialité et la protection des données à caractère personnel, la possibilité de mettre fin à l'entretien à tout moment, la finalité de la récolte de données ainsi que la procédure suivie dans le

cadre de cette recherche a été fourni aux participants en amont de l'entretien afin qu'ils puissent en prendre connaissance.
Tous les participants ont donné leur accord pour que l'entretien fasse l'objet d'un enregistrement audio à des fins de retranscription. Les supports de stockage ont été sécurisés et rendus accessibles uniquement à la chercheuse. Aucun élément permettant de reconnaitre des incidents opérationnels précis, des collègues ou des situations judiciaires en cours n'a été conservé afin d'éviter tout risque pour les participants ou pour la confidentialité des opérations policières.

3.4 Outil de récolte

Pour récolter nos données, nous avons choisi de mener des entretiens individuels semi-directifs (Fugier, 2010). Ces derniers ont été menés par le biais d'un guide d'entretien composé de questions classées par thématiques. Notre volonté était de réaliser un questionnaire qui partait du général pour en arriver au spécifique. Ce choix se justifie par le caractère novateur de la technologie étudiée. En effet, dans la mesure où le cadre juridique belge ne prévoit pas encore l'utilisation de caméras associées à des algorithmes, les zones de police et, par conséquent, leurs fonctionnaires ne sont pas nécessairement confrontés à ces technologies dans leur pratique professionnelle. Nous sommes stratégiquement partis du général afin de contourner d'éventuels refus ou blocages dès le début de l'entretien. L'utilisation d'un guide d'entretien permet de garantir une certaine fiabilité dans la récolte d'information auprès des personnes interrogées (Rondeau et al., 2023). Ce même auteur suggère de recourir à l'entretien lorsque la volonté de la recherche est d'explorer des sujets qui le sont peu. Puisque notre volonté est de s'intéresser aux perceptions qu'ont les fonctionnaires de police à propos des caméras augmentées, cet outil de récolte s'y prête parfaitement.

En fin d'entretien, nous avons posé des questions permettant aux personnes interrogées de synthétiser leurs propos. De plus, nous avons veillé à leur laisser la possibilité de poser des questions. De même, nous leur avons proposé d'éventuellement mentionner un thème que nous n'avions pas balisé et qu'il leur semblerait pertinent d'aborder. Cela nous a permis de nous assurer que notre questionnaire balisait bien l'ensemble du sujet que nous souhaitions traiter. Nous ne manquons pas de remercier la personne interrogée pour sa participation.

3.5 Positionnement de la chercheuse

La chercheuse a adopté un positionnement semi-directif (Fugier, 2010) et neutre en cohérence avec les principes fondamentaux de l'entretien qualitatif (Blanchet & Gotman, 2007 cité par Proulx & Dionne, 2010). L'objectif est d'encourager les participants à développer librement leurs idées, d'éviter d'induire des réponses par des formulations trop orientées, de maintenir une attitude d'écoute active (Heyman, 2024) et d'instaurer un climat d'échange serein.

Ce raisonnement s'inscrit dans l'approche réflexive du chercheur qui reconnait l'influence de sa présence, de ses actions et de ses représentations sur le déroulement de l'entretien (Paillé & Mucchielli, 2021).

4. Résultats

Conformément à l'analyse thématique inspirée des travaux de Pierre Paillé et d'Alex Mucchielli, les données ont été organisées autour de thèmes centraux et récurrents dans les discours. Les résultats seront donc présentés selon quartes axes.

4.1 Gouvernance, cadre normatif et conditions de légitimité

4.1.1 Une gouvernance « multicouche » et un cadre mouvant

Les entretiens réalisés mettent en évidence une perception largement partagée de la complexité du cadre de gouvernance entourant l'utilisation des caméras augmentées au sein des services de police locale.

Les participants décrivent un environnement normatif composé de multiples niveaux réglementaires mêlant dispositions nationales, exigences européennes, règles relatives à la protection des données ainsi que des cadres spécifiques applicables aux pratiques policières. La loi sur la fonction de police est fréquemment citée comme référence centrale pour l'utilisation des caméras par les services de police. Certains rappellent que depuis 2018, on ne parle plus juridiquement de « caméra de surveillance » mais de « caméras » (P1). Cette architecture normative est présentée comme évolutive et parfois incertaine, en particulier dans un contexte marqué par le développement rapide des technologies d'intelligence artificielle. Cette d'instabilité normative est décrite comme susceptible de compliquer la mise en œuvre opérationnelle de certains dispositifs. Quelques participants font notamment référence à des interprétations variables des règles entre zones de police pouvant ainsi mener à des pratiques hétérogènes selon les contextes locaux.

Certains participants insistent sur la difficulté de maintenir une séparation stable entre police administrative et police judiciaire car cette frontière est présentée comme facilement franchissable dans la pratique comme l'explique le participant 1 « pour une zone de police, vous pouvez passer très facilement de la police administrative à la police judiciaire et de la police judiciaire à la police administrative. Et donc le fonctionnaire de police sur le terrain ou un opérateur qui est derrière un écran pour les caméras il va peut-être être dans un premier temps en train de faire de la police administrative mais deux secondes après toujours derrière la même caméra il fera peut-être de la police judiciaire ».

Dans plusieurs zones, la gouvernance est décrite comme associant de nombreux acteurs tels que par exemple les autorités communales et les services et partenaires externes comme des fournisseurs privés. L'idée d'un « dispositif intégré » transparait notamment dans les propos du participant 5 pour qui la demande d'une vision globale s'inscrit dans un échange entre les disciplines afin d'éviter par exemple des conflits de mobilité. « Si on bloque nous des rues mais que les pompiers doivent passer, ils sont confrontés ou engouffrés dans une manifestation revendicative ce qui n'est pas le but. Donc chez nous on a un partenariat avec toutes les disciplines pour avoir une image tout à fait globale ».

Cette perception d'une gouvernance « multicouche » s'accompagne également d'une volonté récurrente d'encadrer le développement technologique plutôt que de s'y opposer frontalement. Plusieurs participants défendent l'idée d'une innovation technologique devant être intégrée dans un cadre de conformité juridique et éthique strict, notamment à travers une logique de « privacy by design » et d'analyse de risques au préalable. Dans cette optique, certains participants soulignent l'intérêt des « sandbox regulatory » qui sont décrites comme « des environnements que les états mettent à disposition des entreprises, du service public pour développer des projets dont on va évaluer l'impact technique, juridique, sécuritaire heu tous les impacts sans risquer de sanctions » (participant 2).

4.1.2 La recherche d'un encadrement conforme au principe de « privacy by design »

La légitimité de dispositifs d'IA de manière générale est fréquemment conditionnée à l'intégration, dès la conception, d'exigences juridiques et éthiques afin de limiter les risques d'usages abusifs ou disproportionnés. A cet égard, il est fréquemment fait référence dans les entretiens, à des outils de contrôle et d'évaluation préalables, tels que les analyses d'impact relatives à la protection des données (DPIA), qui sont décrites comme une étape structurante et systématique avant le déploiement notamment lorsque les technologies sont qualifiées « de nouvelles ou susceptibles d'avoir un impact important » (P1), ainsi qu'aux mécanismes d'évaluation des risques pour les droits fondamentaux. Dans cette logique, l'utilisation de caméras et « l'ajout d'une couche d'intelligence » n'est pas formulé comme un simple choix technique mais comme un processus conditionné par des étapes de conformité. Néanmoins, un contraste ressort dans les perceptions du cadre réglementaire. Certains décrivent un cadre relativement flexible, régulièrement modifié comme dernièrement avec l'insertion des bodycams (P4),

tandis que d'autres soulignent la difficulté de maintenir un cadre règlementaire pleinement adapté à l'évolution rapide des technologies, évoquant parfois un risque de désuétude des normes existantes face à l'innovation technologique (P8). D'autres encore évoquent l'absence d'« un cadre belge pour l'IA » (P2) concourant à freiner l'intégration des dispositifs. « Des zones de polices sont en train de tester ces outils, notre zone de police est en train de tester aussi et tout le monde dit oui il faut qu'on utilise mais il n'y a pas de cadre légal » (P5).

4.1.3 La traçabilité et le contrôle comme garanties de responsabilisation

La traçabilité apparait comme un élément transversal des entretiens. Certains considèrent que les dispositifs de journalisation des accès, les registres de consultation, une justification par numéro de PV ou encore les limitations d'accès aux images constituent des garanties essentielles visant à prévenir les abus internes et à renforcer la responsabilisation des utilisateurs. Dans cette perspective, la surveillance des usages des dispositifs caméra apparait comme un élément central de légitimation. Il semble nécessaire de pouvoir retracer les consultations effectuées par les opérateurs ainsi que d'encadrer strictement les conditions d'accès aux données et aux images des caméras classiques mais également des potentielles caméras augmentées. Ainsi, nous retrouvons une logique de contrôle interne particulièrement présente dans les représentations des participants. Pour certains, l'acceptabilité des technologies de surveillance dépend également de la capacité des institutions policières à garantir un usage encadré et vérifiable des outils déployés. Notons qu'il s'agit d'une obligation légale car la LFP impose la tenue d'un registre de traçabilité. Plusieurs participants expliquent que chaque consultation est notée avec « date, matricule, dossier » et objet de recherche (P10). Certaines caméras disposent d'un système de « log in » visant à vérifier « quelles images ont été consultées et dans quel cadre » (P3). Ces consultations sont susceptibles de faire l'objet d'un contrôle comme l'explique le participant 10 « on sait qui a consulté quoi, quand et comment et de temps en temps moi je fais un petit sondage en demandant tiens à telle heure tu as consulté ça, pourquoi ? Donc comme ça ils savent qu'ils doivent faire attention. […] Il y a la pression sociale, la pression du groupe ». Si la traçabilité est présentée comme une obligation claire, certains soulignent tout de même l'existence de variations de pratiques selon les zones et les services, allant d'une rigueur stricte à des approches plus souples (P3).

4.1.4 Transparence, communication et acceptabilité des dispositifs

L'information du public est présentée comme un levier de légitimité et d'acceptabilité. Plusieurs participants associent la transparence à une exigence démocratique comme le souligne le participant 12 « la population a besoin de transparence, qui plus est avec des outils aussi pointus finalement donc oui je pense que c'est vraiment important qu'on soit transparent par rapport à la localisation et l'usage [des systèmes caméras] ». La présence de pictogrammes et la communication institutionnelle sont décrites comme des éléments essentiels de l'intégration sociale des dispositifs. Certains participants évoquent la nécessité de trouver un équilibre entre les impératifs de transparence démocratique et les contraintes opérationnelles propres aux activités policières, notamment en matière de sécurité ou d'efficacité des dispositifs.

Les discours recueillis font apparaitre des retours variables de la part des citoyens. Certains participants rapportent une évolution dans le temps allant d'une opposition initiale « vous allez nous espionner » à une demande d'extension « les gens demandent plus de caméras » (P2). D'autres, au contraire, signalent peu de retours directs, la caméra étant devenue un élément du paysage auquel on ne prête plus attention (P6, P12). Dès lors, la caméra est présentée comme un outil qui rassure certains habitants mais elle peut également être associée au sentiment d'être trop surveillé. L'acceptabilité apparait donc comme contextuelle et non uniforme, dépendant des quartiers, des expériences et du rapport à l'institution.

4.1.5 Vers une harmonisation des pratiques et des cadres d'utilisation

Certains participants évoquent une volonté de standardisation des procédures, des mécanismes de contrôle et des cadres d'utilisation afin de réduire les disparités observées sur le terrain. Ainsi, le participant 3 illustre cela avec un exemple concret « nous on permet un rétroacte de 15 minutes. Dans certaines zones, c'est illimité et dans d'autres c'est uniquement en live donc ça dépend vraiment de la décision du chef de corps et de son approche et son interprétation de la loi ». La nécessité d'égalité de traitement sur le territoire, indépendamment de la zone de police, est formulée explicitement par le participant 1, il serait souhaitable que « quelqu'un qui soit confronté à un service de police à X ou à X [noms de zones] soit traité de la même manière par rapport à l'utilisation de cet outil ». D'autres participants complètent en évoquant des besoins de coordination accrue à l'échelle européenne, particulièrement dans un contexte marqué par la circulation transfrontalière des individus, des données et des menaces sécuritaires. Cette recherche d'harmonisation apparait comme une tentative de concilier innovation technologique, sécurité juridique et cohérence opérationnelle au sein des pratiques policières contemporaines.

4.2 Les usages et finalités de l'utilisation des caméras augmentées dans les pratiques policières

4.2.1 Les caméras augmentées comme outils de gestion de l'ordre public

Les participants associent l'utilisation de caméras augmentées à une amélioration des capacités de gestion de l'ordre publique, notamment dans le cadre d'évènements à forte affluence. Les participants évoquent par exemple l'intérêt des dispositifs pour la gestion des flux, l'observation des mouvements de foule ainsi que l'anticipation de certaines situations susceptibles de nécessiter une intervention policière. Plusieurs participants décrivent les systèmes caméras comme des outils permettant d'obtenir une vision plus globale et plus dynamique de l'espace public. Cette capacité de visualisation élargie apparait comme un élément favorisant la coordination des dispositifs policiers et l'adaptation plus rapide des réponses opérationnelles en fonction de l'évolution de la situation sur le terrain. L'intérêt des fonctionnalités automatisées de comptage ou de détection dans certains contextes spécifiques, notamment lors de rassemblements, d'évènements festifs ou de manifestations publiques est mis en avant dans le corpus. Certains participants, comme le participant 6, considèrent que ces technologies permettent de soutenir les capacités d'analyse des opérateurs humains face à des environnements caractérisés par une forte densité d'information visuelles. « Évidemment, on s'aide aussi des caméras de surveillance qui sont un outil qui est devenu incontournable puisque ça permet de surveiller de grandes zones en même temps, d'anticiper les mouvements de foules de supporters et de diriger aux mieux nos équipes car quand vous êtes dans une foule de 6000 personnes qui viennent de toute part, les effectifs sur le terrain ont tout de suite une vue plus restreinte donc les cameras ça permet de prendre de la hauteur ». De manière plus générale, les participants tendent à présenter les caméras, le cas échéant associées à des algorithmes, comme un outil d'aide à la décision permettant d'améliorer la réactivité des services de police dans le cadre du maintien de l'ordre public. Les participants insistent également sur le fait que les caméras permettent d'attirer l'attention sur un évènement, signaler un flux ou une densité mais sans se substituer à l'évaluation humaine. Le participant 2 met en avant la possibilité, grâce aux caméras, de surveiller sans augmenter la présence visible de policiers ce qui tend à favoriser une logique de désescalade.

4.2.2 Un soutien opérationnel durant les interventions policières

L'appui à l'intervention constitue un usage central des caméras. Les participants soulignent notamment l'intérêt des dispositifs pour améliorer la connaissance situationnelle des équipes engagées sur le terrain et faciliter la coordination entre les différents acteurs mobilisés. Le participant 11 explique qu'« on n'intervient pas de la même façon si on a des images ou si on n'en a pas ». Les caméras permettent

notamment de vérifier les informations provenant d'un appel et ainsi réduire le décalage entre ce qui est rapporté par téléphone et la situation réelle, d'estimer le nombre de personnes, de repérer des directions de fuite, d'observer la présence d'armes. « L'algorithme pourrait nous indiquer si effectivement c'est dangereux, s'il y a des armes etc ». Cela pourrait également permettre d'« être prévenu directement, avant que les gens nous appellent » (P11). Ces usages ainsi que l'accès à des informations en temps réel permettraient donc de renforcer la capacité d'évaluation des risques avant ou pendant une intervention. Dans cette perspective, les caméras sont explicitement associées à une amélioration de la sécurité des équipes policières. De plus, certains participants évoquent également l'utilité des systèmes pour identifier plus rapidement des besoins de renforts ou orienter les effectifs disponibles en fonction de l'évolution de la situation comme l'explique le participant 6 « ça renforce la sécurité des intervenants aussi et ça c'est quand même un point non négligeable. Quand dans le cadre du foot vous voyez qu'il y a un groupe d'une cinquantaine de personnes qui arrivent cagoulées avec des bouteilles en verre cassées en main, avec des barres en fer et que ce groupe arrive vers un certain point de contrôle, vous savez qu'il est grand temps d'envoyer des renforts pour renforcer ce point de contrôle ». Les discours mettent en évidence une logique d'optimisation opérationnelle reposant sur une circulation plus rapide de l'information et sur une capacité accrue de coordination des interventions. Les caméras augmentées sont fréquemment envisagées comme une extension de cette logique en ce sens que la machine pourrait sélectionner « les bonnes caméras aux bons moments » lorsque les yeux humains ne suffisent pas (P6).

4.2.3 L'accélération de l'exploitation des images dans les enquêtes

Bien que l'objet principal de cette recherche soit l'intégration des caméras dites augmentées dans le cadre de la police administrative, nous constatons que l'un des apports les plus fréquemment évoqués par les participants concerne l'exploitation des images à des fins d'enquête. Les participants décrivent ces technologies comme un outil permettant de faciliter et d'accélérer le traitement de volumes importants de données vidéo, particulièrement dans des contextes où les capacités humaines apparaissent limitées face à la quantité d'images disponibles. « Je n'ai pas fait d'analyse mais une vidéo qui dure 30 min, il faut compter une journée d'exploitation quoi. Il faut la regarder, attendre le bon moment, faire une capture d'écran, sortir cette capture d'écran, l'annoter, vérifier que, l'annexer au pv donc voilà ça prend vraiment beaucoup de temps » (P11). Le participant 6 rejoint cette idée de gain de temps « les outils actuels d'intelligence artificielle qui existent sur le marché nous n'en disposons pas et donc ce sont les humains qui font le boulot avec une perte de temps incroyable ». En outre, le participant 7 renforce l'idée que l'IA a sa place lorsque le traitement d'un volume d'informations dépasse les capacités humaines « ça, [le métier de ceux qui font les analyses criminelles opérationnelles] demain, l'IA, à mon sens, elle doit remplacer. Ça, ça fonctionnait tant que le volume des données était à taille humaine. Il ne l'est déjà plus ». Plusieurs participants expliquent que les fonctionnalités algorithmiques permettent d'effectuer un premier tri des images, de filtrer des séquences pertinentes ou encore de chercher des individus sur base de caractéristiques spécifiques. Cela représente un intérêt notamment dans les situations nécessitant d'analyser un grand nombre d'heures d'enregistrement. L'intérêt accordé aux fonctions de restitution de parcours ou de suivi d'itinéraires dans le cadre d'investigations est également souligné. Les caméras associées aux algorithmes sont donc fréquemment présentées comme un « accélérateur » de l'exploitation des images plutôt que comme un substitut au travail d'enquête. Rappelons que les entretiens révèlent une certaine porosité entre les usages relevant du maintien de l'ordre public et ceux associés à la police judiciaire. Certains dispositifs peuvent être initialement déployés dans une logique de gestion administrative de l'espace public mais les données peuvent aussi présenter un intérêt dans le cadre d'investigations judiciaires comme l'explique le participant 5 « on a [dans les images] un crime qui s'est passé et pouvoir utiliser un système intelligent c'est utile à l'enquêteur ». Le participant 12 illustre l'apport des caméras pour l'enquête, « on a été confronté, on l'est toujours mais dans de moindres mesures, à du deal de rues. […] On avait des dealers qui vendaient

alors qu'il y avait une caméra juste au-dessus de leurs têtes. Donc ça ne les a jamais empêchés. Par contre, une fois qu'on les interpellait, les images caméras permettaient d'alimenter le dossier et de garantir d'avoir une peine au niveau de la justice ».

4.2.4 Des effets préventifs perçus comme relatifs et contextuels

Les participants attribuent un potentiel préventif ou dissuasif aux caméras augmentées, tout en nuançant fortement la portée réelle de ces effets en matière de réduction de la criminalité ou des incivilités. Selon le participant 1, « il serait illusoire de croire que c'est la réponse à tout. C'est un moyen parmi d'autres, ce n'est pas la panacée ». Certains considèrent que les bénéfices au niveau préventif dépendent du contexte d'utilisation des dispositifs, notamment leur visibilité, de la qualité de la communication autour de leur présence ou encore de l'existence d'une présence policière effective sur le terrain. Pour le participant 5, le coté préventif est rattaché à la capacité d'envoyer une patrouille en cas de suspicion sur les images caméras « si on voit la nuit un attroupement de jeune place X, on peut y aller, en accord avec notre dispatching, on peut envoyer des patrouilles en préventif sur place ». La technologie apparait donc rarement suffisante à elle seule pour produire des effets dissuasifs durables. La majorité des participants évoquent le risque de déplacement de certaines formes de délinquance vers des zones moins surveillées tendant ainsi à limiter l'impact global des dispositifs sur les phénomènes criminels observés. « Quand vous installez des caméras, vous avez trois conséquences possibles. C'est un déplacement dans l'espace, vous avez un déplacement éventuellement dans le temps donc c'est se dire il y a des caméras donc je vais faire ça le soir quand il fait noir ou alors vous avez des déplacements en fonction de la nature du fait. Ça veut dire que d'un type de fait, vous passez à un autre type de fait » (P1). D'autres soulignent la difficulté d'objectiver de manière précise les effets réels des caméras augmentées sur la criminalité ou le sentiment de sécurité. « C'est à voir en fonction de à qui on pose la question. Par exemple, quelqu'un de plus à gauche va dire il y a trop de surveillance et quelqu'un de plus à droite va dire il faut plus de caméras. Ça dépend de si c'est quelqu'un qui est à l'aise avec les caméras ou non. Ça dépend de la population, si on va dans des quartiers plus aisés comme le quartier X on va nous dire oui il faut plus de caméras mais si on va dans des quartiers plus démunis, on va nous dire il y a trop de caméras […]. Il y a plus de sentiment de persécution dans ces quartiers » (P5).

4.2.5 L'intelligence artificielle comme outil de rationalisation organisationnelle

Au-delà des usages directement liés aux caméras augmentées, plusieurs participants évoquent plus largement le potentiel de l'IA dans les pratiques policières quotidiennes, notamment en mettant en évidence des attentes liées à l'automatisation de certaines tâches administratives ou répétitives considérées comme particulièrement chronophages. Les participants mentionnent par exemple des usages liés à l'aide à la rédaction, à la retranscription ou encore à l'analyse documentaire. Cela pourrait, entre autres, permettre une meilleure allocation des ressources humaines disponibles. Cela permettrait aussi de dégager du temps pour l'opérationnel comme l'explique le participant 4 « je ne demande que ça moi qu'on puisse développer l'IA au sein de la police pour pouvoir soulager les collègues opérationnels que ce soit au niveau caméras ou dans d'autres domaines hein. Il y a des tâches administratives qui demandent beaucoup de temps et d'énergie […]. En tant que citoyen on demande du bleu dans les rues. Donc si on peut faciliter les tâches administratives pour pouvoir permettre au policier d'être dans les rues ben je pense qu'on aura tout gagné et je pense que l'IA va permettre ça ». Pour certains, l'IA pourrait également être un vecteur de standardisation de certaines pratiques ou procédures internes permettant ainsi d'améliorer l'efficacité organisationnelle des services de police. Toutefois, les participants demeurent prudents quant à la place qui pourrait être accordée à ces outils. Il s'agirait davantage d'un soutien technique destiné à assister les professionnels plutôt qu'à se substituer à leur expertise et leur pouvoir d'appréciation.

4.3 Limites techniques et défis opérationnels de l'intégration de caméras augmentées

4.3.1 Des contraintes financières et infrastructurelles importantes

Les entretiens réalisés mettent en évidence que le déploiement des dispositifs de caméras s'accompagne de contraintes financières et matérielles. Le participant 10 explique que « les limites, ce sont les limites budgétaires parce que ça a un coût. On est presque à un million d'euros au total » pour des caméras « classiques ». Concernant l'intégration de caméras augmentées, il expose « ça se développe. On est approché par plusieurs personnes mais ça coûte déjà très cher ». Le coût élevé associé à l'acquisition des infrastructures technologiques, à leur maintenance ainsi qu'au stockage des données générées par les systèmes caméras apparait comme un obstacle transversal. Les dépenses liées aux licences, aux mises à jour ainsi qu'au renouvellement progressif des équipements devenus obsolètes sont également mentionnées. De plus, certains participants expliquent que certaines caméras initialement installées ne disposent pas des capacités techniques pour supporter les nouveaux outils algorithmiques. Cela implique dès lors des investissements supplémentaires.

Plusieurs participants évoquent l'existence d'inégalités entre zones de police quant aux capacités financières et techniques permettant le développement de tels dispositifs. Les discours recueillis montrent que les ressources disponibles influencent fortement les possibilités concrètes de mise en œuvre des technologies intégrant l'intelligence artificielle au niveau local. « Je pense néanmoins qu'on est quand même fort en retard notamment dans certaines zones où il y a peu de budget. Par rapport au privé ou par rapport à des zones de polices qui mettent le paquet et la référence en la matière c'est quand même Anvers qui est une zone locale avec des moyens colossaux en développement informatique » (P6).

4.3.2 Des contraintes humaines et organisationnelles persistantes

Sur le plan humain, certains insistent sur le besoin de disposer de profils techniques et spécialisés capables d'assurer la gestion, le paramétrage ainsi que le suivi des systèmes déployés. D'autres évoquent également une potentielle augmentation de la charge de travail liée au traitement des alertes générées par les dispositifs algorithmiques. L'argument étant le risque de multiplication des sollicitations nécessitant une vérification ou une intervention humaine dans un contexte où les ressources opérationnelles peuvent être limitées. Le participant 8 décrit l'analyse vidéo comme « un train qui ne s'arrête jamais » car « si vous mettez de la détection en route il faut se dire qu'en fonction du nombre de caméras que vous avez et du nombre de scénarios que vous avez encodé, ça va sonner tout le temps ». Il souligne également l'écart entre la satisfaction hiérarchique et les contraintes opérationnelles « au niveau +1, ils sont super contents parce que l'outil fonctionne mais au niveau -1 ils en bavent parce qu'il ne faut pas oublier que y a tout le travail [de traitement des alertes] derrière ». Toutefois, la plupart des participants mettent en avant le fait que les outils algorithmiques pourraient contribuer à atténuer certaines contraintes déjà rencontrées dans l'exploitation classique des images caméras. En effet, ces outils pourraient pallier aux difficultés liées à la surcharge cognitive des opérateurs, à la fatigue, à la capacité du cerveau humain à focaliser son attention sur une tâche durant une longue période ou encore à la capacité limitée des individus à surveiller simultanément un nombre important de flux vidéo. Le participant 6 évoque « un gain de temps énorme et un gain d'efficacité parce que l'opérateur s'il se retourne pour prendre sa bouteille d'eau pendant deux secondes ou s'il éternue ben il se peut qu'il loupe une info. La machine elle ne le loupera pas ». Les discours révèlent ainsi une ambivalence, l'outil promet un gain de temps mais peut déplacer la charge vers le traitement d'alertes et la gestion de faux positifs. Par ailleurs, le participant 11 exposent un enjeu managérial dans l'intégration des nouvelles technologies au sein de la police en partie dû au mix générationnel. « On a selon les services, 5 générations qui travaillent en même temps quoi. Clairement d'un point de vue managérial je ne gère pas de la même façon quelqu'un de 58 ans qui est à deux de la pension qu'un de 19 ans qui sort de l'école […] tout ce

qui est caméra, bodycam etc ben plus on va avancer et plus ça va être facile car on a une génération connectée qui vit avec tout ça et qui n'a pas de mal à intégrer cette notion-là ».

4.3.3 Les limites liées à la qualité des données et au paramétrage des systèmes

L'efficacité et la fiabilité des dispositifs de caméras augmentées sont décrites comme fortement dépendantes de la qualité des données exploitées ainsi que du paramétrage des systèmes utilisés. Différents facteurs techniques tels que l'angle de la caméra, les conditions météo, la luminosité etc., sont cités comme pouvant influencer la fiabilité des analyses produites. Plusieurs participants expliquent également que des données de mauvaise qualité peuvent entrainer des résultats erronés ou pas pertinents selon le principe du « garbage in, garbage out ». Ces différents points sont notamment illustrés par le participant 11 dans l'exemple des caméras ANPR. « Je pense que c'est une plus-value avec le biais que la qualité des images doit être impeccable sinon ça ne marche pas. On a des caméras ANPR et on a déjà ce soucis-là. Parfois la caméra détecte une plaque déclarée comme volée ou on nous annonce un fait judiciaire important et quand on arrive sur place on se rend compte que la caméra a pris un 6 pour un 8 et que la personne n'a rien demandé et se fait braquer par 3 combis alors que c'est une mauvaise lecture de la plaque ». Il subsiste des risques de faux positifs. Nous observons donc au sein des discours que les performances des technologies dépendent des conditions concrètes d'utilisation et de la qualité des infrastructures disponibles.

4.3.4 Le maintien de l'humain au cœur du processus décisionnel

L'un des constats les plus récurrents dans les entretiens concerne l'importance accordée au maintien de l'humain et de sa capacité de contrôle dans l'utilisation des dispositifs technologiques et notamment ceux relatifs aux caméras augmentées. Les participants insistent sur le fait que les outils d'IA doivent être envisagés comme des mécanismes d'aide à la décision humaine plutôt que comme des systèmes autonomes. Ainsi, les discours évoquent la nécessité d'une « levée de doute » humaine avant toute décision opérationnelle fondée sur une alerte ou une analyse générée par un système algorithmique. « Je ne conçois pas une intelligence artificielle qui soit autonome. La décision doit appartenir à l'être humain. Et c'est prévu ainsi dans la loi belge et dans l'IA Act surtout dans les systèmes à haut risque et c'est très bien. On ne peut pas se dire on va confier le dernier mot à des robots. La technologie n'est pas prête pour ça, la société non plus […]. Donc un contrôle et une supervision humaine toujours ! Moi je vois ça comme un outil d'aide, une assistance » (P2). D'autant que les outils algorithmiques ne disposent pas de la capacité d'interprétation contextuelle ou du jugement nécessaire pour remplacer l'appréciation humaine dans des situations complexes rencontrées sur le terrain comme l'illustre le participant 8 « prenons un autre exemple pour vraiment vous faire comprendre que ce n'est pas l'IA qui va solutionner le monde mais plutôt cette levée de doute. Imaginons un véhicule dans une rue à contre sens un lundi à 8h00 du matin, ben c'est peut-être quelqu'un qui s'est trompé de chemin. Un vendredi soir de grosses festivités, un véhicule qui se présente dans une rue où il n'est pas attendu, là je peux vous dire que les policiers ont les poils qui se dressent et se demandent ce qu'on fait ». L'exigence d'attribuer un rôle central à l'humain apparait comme particulièrement importante dans des contextes susceptibles d'entrainer des conséquences significatives pour les individus concernés. Il y a également une nécessité de formation des personnes susceptibles d'utiliser les systèmes caméras. « Le fait que les gens soient correctement formés à l'utilisation de l'outil c'est important et c'est aussi un risque si ça ne l'est pas. Parce que la supervision humaine c'est important mais il faut une supervision humaine avec des formations qui sont correctes car si les gens ne comprennent pas les outils et qu'ils les utilisent mal, ça ne va pas non plus donner de bons résultats » (P2).

4.3.5 Dépendance aux infrastructures et impact environnemental

Les entretiens montrent qu'il y a une dépendance structurelle des dispositifs caméras à des infrastructures techniques robustes. Au-delà des performances des logiciels, l'efficacité opérationnelles

de ces systèmes repose sur la continuité de chaines matérielles (alimentation électrique, réseaux de télécommunication, connectivité des serveurs, capacité de stockage) dont la fragilité peut paralyser l'outil. Plusieurs participants soulignent que l'intégration de technologies accroit la vulnérabilité des services en cas de défaillance infrastructurelle. Cette préoccupation est formulée explicitement par le participant 2 « Il faut quand même bien garder à l'esprit que on bombarde des technologies de tout coté mais ce sont des technologies qui dépendent de l'électricité donc plus de courant, plus d'aide, plus de technologies ». Le participant 10, quant à lui, souligne un enjeu environnemental en rappelant que les infrastructures de stockage « ça a un cout aussi sur l'environnement » et qu'il ne faut pas négliger cet aspect (P10).

4.4 Droits fondamentaux, risques de dérives et rapports de pouvoir

4.4.1 Les risques perçus pour les droits fondamentaux

Les risques pour les droits fondamentaux sont principalement formulés autour du droit au respect de la vie privée, à la protection des données personnelles, la non-discrimination. Certains participants émettent également des inquiétudes quant à une possible fuite des données, un piratage ou des accès non autorisés aux systèmes utilisés par les services de police. De plus, certains participants soulèvent tout de même une inquiétude face à un risque d'usage interne inapproprié des images ou des données ou un risque potentiel d'extension du contrôle dans les espaces publics. A cet effet, ils insistent sur la nécessité de mettre en place un cadre strict d'utilisation de l'outil. « Il faudra mettre en place en interne des mécanismes de gestion des risques par rapport à une utilisation détournée de l'outil vu l'implication que ça peut avoir sur la vie privée des citoyens, ce serait mal venu qu'un policier puisse suivre son épouse dans la rue, etc donc il y aura un cadre à mettre en place par rapport à l'utilisation de l'outil ». (P9). Plusieurs participants pointent également du doigt les risques liés aux biais pouvant affecter les systèmes algorithmiques. Effectivement, il subsiste des préoccupations quant à la qualité des données d'entrainement ainsi que les conséquences de certains biais, statistiques ou structurels, sur les résultats produits par les systèmes. En outre, si des données sont marquées par certaines pratiques policières ou certains déséquilibres sociaux, cela pourrait contribuer à reproduire ou renforcer des formes de discrimination indirecte dans les processus de surveillance ou d'identification. Le participant 5 l'illustre comme ceci « l'algorithme va apprendre sur tout ce qu'on va lui mettre à disposition, sur tout ce qu'on va lui donner comme infos. On a qu'à prendre les statistiques policières chez nous. Les stats disent que 90% des vols à l'étalage, les agressions et les vols avec violences sont toujours commis par un certain type de personnes. Si on va mettre nos stats dans le système, alors le système va apprendre qu'il n'y a qu'un noir, un nord-africain, un Marocain qui commet des vols ou des agressions, ce qui n'est en réalité pas du tout le cas. Mais donc le risque de biais est là-dedans ». Ainsi, il dénonce également le fonctionnement « boite noir » de certains systèmes « personne ne comprend comment le système en arrive à cette conclusion […] et donc ça c'est aussi une difficulté ». D'autres en revanche identifie le risque de discrimination comme étant un argument de débat plus que comme un problème opérationnel et estiment que « le codage pourrait alors se tenir à des choses très factuelles ou alors un encodage très simplifié de l'humain à la base » (P11) afin de minimiser les risques. Cette divergence met en avant une ambivalence entre une approche prudente axée sur la gouvernance et une approche davantage centrée sur la finalité policière « on cherche des gens qui font ce qu'il ne faut pas » (P6).

La protection des données apparait chez les participants comme une condition indispensable pour légitimer les dispositifs technologiques. Le participant 7 explique qu'il faudra veiller au respect des procédures et à rappeler le cadre parce que « l'abus ne sera pas nécessairement volontaire ». Il poursuit en développant « je pense que dans le risque, il faut estimer qu'il y a un risque globalement structurel ou systémique. Il arrivera parce que les gens ne feront pas trop attention. Ce ne sera pas forcément le gars qui voudra commettre une faute ». Au vu de ces craintes, les participants insistent, à nouveau, sur l'importance d'avoir des mécanismes de contrôle humain, des évaluations préalables et de la supervision

des systèmes pour limiter les risques. A cet effet, le participant 2 insiste notamment sur le besoin de regulatory sandbox « pour développer des projets dont on va évaluer l'impact technique, juridique, sécuritaire […] sans risquer de sanctions » et ainsi pouvoir adapter la technologie selon les résultats obtenus. En définitive, les résultats mettent en évidence que les participants ont globalement conscience des biais potentiels des technologies et des enjeux pour les droits fondamentaux.

4.4.2 L'acceptabilité sociale comme enjeu politique et sociétal

L'acceptabilité sociale des dispositifs de caméras algorithmiques constitue un enjeu central dans les représentations des participants qui considèrent que leur légitimité dépend de la manière dont ceux-ci sont perçus par la population ainsi que du contexte politique et sécuritaire dans lequel ils sont déployés. Plusieurs participants expliquent à cet effet que des contextes marqués par des attentats, des crises sécuritaires ou des phénomènes de violence peuvent modifier l'acceptation de certaines technologies de surveillance au sein de la population ou des responsables politiques. Les entretiens mettent en évidence l'existence de tensions entre des attentes de sécurité accrues et des préoccupations relatives à la protection des libertés individuelles. Il est dès lors considéré que le développement des technologies algorithmiques nécessite un débat démocratique et politique approfondi concernant les limites acceptables de son usage au sein de l'espace public car, selon les participants, il y a une polarisation possible des perceptions citoyennes. Selon le participant 2, plus l'outil est perçu comme « boite noire », plus il est susceptible d'ouvrir la porte à des hypothèses et des craintes. A l'inverse, la communication et la transparence sont décrites comme un moyen de renforcer la confiance. L'acceptabilité apparait donc comme un enjeu à la fois technique, ce que fait l'outil, et politique, comment il est discuté et encadré.

4.4.3 Les usages perçus comme disproportionnés ou inacceptables

Certains usages sont jugés comme difficilement acceptables ou disproportionnés pour certains participants. Ces derniers soulèvent notamment des inquiétudes quant au risque d'une surveillance généralisée de l'espace public, associée à une collecte massive et centralisée de données permettant ainsi le suivi des déplacements ou des comportements des citoyens. Les technologies biométriques et plus particulièrement la reconnaissance faciale occupent une place importante dans le discours des participants. Cependant, les positions sont nuancées selon les participants et selon les contextes envisagés. Certains considèrent que de tels outils pourraient être acceptables dans des situations exceptionnelles et bien définies telle que la lutte contre le terrorisme ou dans le cadre de menace graves pour la sécurité publique. Par ailleurs, tous les participants s'accordent pour dire qu'ils ne souhaitent pas vivre dans une société où tout est surveillé comme l'explique le participant 1 « j'en parle à l'aise en tant que commande des services de police, je ne voudrais pas vivre dans un monde où on est filmé en permanence ». Les technologies de prédiction de comportements font également l'objet d'inquiétudes et les participants adoptent une position prudente à leur égard.

4.4.4 Dépendance technologique, souveraineté et rôle du secteur privé

Les moyens financiers et les compétences techniques nécessaires au fonctionnement des systèmes semblent être détenues, selon les participants, par des acteurs privés. Par conséquent, ces derniers interviennent dans le développement, la fourniture ou la maintenance des dispositifs technologiques. Certains participants mettent en avant des inquiétudes concernant le contrôle effectif des données et des infrastructures utilisées en insistant sur l'importance de conserver une maitrise institutionnelle des serveurs, des accès et des données collectées et ce particulièrement dans un contexte marqué par les enjeux de souveraineté numérique et de cyber sécurité. Le participant 1 illustre ce propos à l'aide d'un exemple « on est allé voir une société pour des caméras fixes temporaires, c'est la même chose, on vous propose des connexions 4G bientôt 5G où vous pouvez vous connecter derrière n'importe quel pc et regarder en ligne les images des caméras. Ça on n'en veut pas, on va le désactiver. On ne veut pas que

ce soit sauvegardé sur un cloud, potentiellement accessible aux fournisseurs et services qui nous mettent à disposition les caméras. Les images sont rapatriées par VPN sous nos serveurs et on fera la consultation sur nos serveurs (P1). Les entretiens montrent une tension où d'un côté le privé est jugé comme indispensable notamment pour disposer d'outils « up to date » (P7) et de l'autre, il est associé à des risques de dépendance, de verrouillage technologique et de perte de souveraineté. « Maintenant, il faut faire attention à l'aspect lobbying aussi. C'est des marchés publics et il ne faudrait pas, selon moi, qu'il y ait une société qui regroupe tout » (P10). Dans cette optique, les participants soulignent différents mécanismes susceptibles de renforcer le contrôle institutionnel des dispositifs technologiques tels que des clauses contractuelles, des mécanismes de contrôle des fournisseurs ou encore le développement de compétences techniques en interne. La question du visionnage des images par des agents du privé est contrastée. Plusieurs participants refusent cette possibilité en soulignant que les agents privés « n'ont pas la même formation » ni « la même approche éthique que les membres de la police » (P3). Le contraste est également mis en avant par rapport aux contrôles des responsabilité. Alors que la police « doit rendre des comptes » et respecter des règles « extrêmement strictes », le recours à des agents sous contrats précaires est décrit comme « l'ouverture à tous les excès » (P2). Enfin, la critique vise la logique économique et ses effets sur le personnel. Selon le participant 8, « même lorsqu'un énorme screening » existe, il ne faut pas négliger les « intérêts commerciaux » et l'instabilité des équipes avec un « turnover de personnes » susceptibles de partir parce « qu'ils auront trouvé une meilleure opportunité financière ailleurs » (P8). Ainsi, selon ce participant, ce type de mission devrait relever de personnes « au service de la communauté, sans intérêt commerciaux ». Le participant 12 quant à lui explique que le privé répond aux besoins auquel le public n'apporte pas de solutions. De plus, il juge le visionnage acceptable si les conditions sont identiques « des données sauvegardées de façon sécure, un cadre pour accéder et un cadre pour exploiter ». Cette position est aussi formulée en termes de contraintes capacitaire « on n'a pas le choix (…) on doit permettre au privé de le faire ». Il existe donc une ambivalence entre une logique de capacité et une logique de légitimité.

5. Discussion

Les résultats tendent à confirmer que l'intégration de l'IA dans les pratiques policières, notamment par le biais des caméras augmentées, ne constitue pas uniquement une évolution technique. Cette évolution semble également s'accompagner d'une reconfiguration plus large des pratiques de surveillance, des logiques sécuritaires et des rapports de pouvoir, pouvant varier selon les contextes institutionnels et les modalités concrètes d'utilisation. Les résultats vont globalement dans le sens de la littérature et montrent que les participants ont conscience des enjeux et des défis que soulèvent ces nouvelles technologies.

L'encadrement des dispositifs est tantôt perçu, par les participants, comme protecteur et actualisé et tantôt comme insuffisant ou en retard. L'importance accordée à la gouvernance et à l'encadrement normatif des dispositifs qui transparait dans les discours rejoint les réflexions développées par Marina Teller (2024). Selon elle, la régulation de l'IA constitue une condition essentielle au maintien des équilibres sociétaux, démocratiques et politiques. L'intelligence artificielle soulève des enjeux techniques mais interroge aussi les valeurs collectives et les droits fondamentaux dans les sociétés démocratiques. L'auteur défend l'idée que le droit ne doit pas intervenir de manière réactive mais devrait plutôt participer activement, aux côtés des acteurs techniques et scientifiques, à la définition des normes et valeurs encadrant les dispositifs. Dans le même sens, les résultats montrent une recherche de conformité en accord avec le principe de « privacy by design » développé par Ann Cavoukian (2012). Les participants vont dans le même sens que l'auteur et estiment que les garanties relatives aux droits fondamentaux doivent être intégrées dès la conception des systèmes technologiques. Pour que les fournisseurs puissent « contrôler leurs produits et leurs innovations sans ressentir le plein pouvoir de

l'appareil de régulation étatique », l'IA Act vise à rendre obligatoire la mise en place de « regulatory sandbox». Cette période d'essai en conditions réelles permet « d'innover tout en garantissant la conformité » (Trstenjak, 2024, p. 11). Le but des sandbox étant d'identifier les éventuels risques engendrés par l'IA. Toutefois, certains auteurs émettent des réserves notamment face à un potentiel risque de mise en application des sandbox de manière inégale entre les États membres (Trstenjak, 2024).

Les travaux de Michel Foucault (1975) sur les mécanismes disciplinaires permettent notamment de comprendre comment les dispositifs de surveillance peuvent contribuer à transformer les comportements sociaux par la visibilité permanente des individus. En effet, cet auteur se réfère au modèle du panoptique développé par Bentham qui illustre que les individus, en sachant qu'ils peuvent être surveillés à tout moment, finissent par exercer une forme d'auto contrôle. La théorie criminologique de la vitre brisée développée par Wilson et Kelling (1982) peut également être mobilisée afin de comprendre certaines politiques de sécurité encourageant notamment l'augmentation de la surveillance de certains espaces publics afin de détecter rapidement des incivilités et ainsi de prévenir une potentielle escalade vers des infractions plus graves. De plus, les discours médiatiques tendent à renforcer l'idée d'un besoin de sécurisation des espaces publics (Charlier et al., 2025). Toutefois, les résultats montrent que les effets préventifs des caméras augmentées sont considérés comme relatifs et contextualisés. Les effets préventifs seraient liés au pouvoir symbolique des caméras qui contribueraient à transmettre l'idée que certains espaces sont protégés ou plus surs, ce qui pourrait modifier les perceptions et les comportements des individus dans ces lieux (Kaenzig & Klauser, 2018).

Cependant, certaines études montrent que l'efficacité des caméras en matière de prévention varie selon les contextes et les formes de criminalité. Les dispositifs semblent produire plus de résultats en matière d'infractions contre les biens que contre les personnes (Gill & Spriggs, 2005). Ceci tend à s'expliquer par le fait que les caméras agissent davantage sur la criminalité rationnelle que sur la criminalité émotionnelle. Ainsi, il y aurait peu d'effets dissuasifs sur les comportements impulsifs comme le vandalisme, les agressions ou encore les troubles à l'ordre public sous substances psychotropes (Kaenzig & Klauser, 2018). Par ailleurs, les délinquants tendent à « s'accoutumer à la présence de caméras et finissent par les oublier » réduisant donc la dissuasion sur le long terme (Kaenzig & Klauser, 2018, p. 65). Welsh et Farrington (2002) exposent que les caméras peuvent également provoquer deux phénomènes, une diffusion des bénéfices, ou un déplacement de la criminalité (temporel, tactique, ciblé, territorial et fonctionnel). Dans leur étude, Kaenzig et Klauser (2018), mettent en évidence qu'il n'y a pas de diminution significative de la criminalité suite à la mise en place du réseau de caméra. En revanche, elles observent tout de même un effet de déplacement, dans les rues voisines, en matière de faits de stupéfiants. Cependant, malgré la présence de caméras, des transactions continuent de se dérouler dans les espaces surveillés.

En raison de la limitation budgétaire de certaines zones, l'intérêt de la mise en place des caméras semble contrebalancé par le coût de celles-ci. L'intérêt apparait donc moindre dans les zones rurales ou semi-rurales. Ce raisonnement suit la logique de priorisation des budgets tel qu'expliqué par le participant 6. Par ailleurs, une logique de priorisation des espaces criminogènes peut également être appliquée conformément à la théorie de la prévention situationnelle (Wyvekens, 2008 ; Australian Institute of Criminology, 2003). De plus, les caméras tendent à être davantage acceptées lorsque qu'elles « contribuent au maintien de l'ordre social et de la sécurité publique dans des lieux jugés à risque parce que criminogènes » (Boudreau et al., 2005 p. 13).

A la lumière des apports théoriques développés ci-dessus, les caméras augmentées doivent être envisagées comme des outils complémentaires au sein de stratégies plus larges de prévention et de

gestion de la sécurité plutôt que comme des solutions autonomes capables de résoudre les phénomènes criminels.

Charlier et al. (2025) rejoignent les propos développés ci-dessus en ce sens qu'ils exposent que le développement des politiques numériques de sécurité urbaine ne s'explique pas uniquement par des enjeux de sécurité publique, mais également par des intérêts économiques, technologiques et politiques liés à l'essor du marché de la sécurité privée et des technologies numériques. Ces évolutions favorisent la commercialisation de dispositifs sécuritaires présentés comme permettant un gain de temps et d'efficacité mais nécessitant des investissements publics et privés, entrainant des lors des débats politiques, juridiques et citoyens. Nos résultats montrent également un rôle effectif et croissant des acteurs privés notamment dans la fourniture et la maintenance des dispositifs technologiques. Des préoccupations liées à la maitrise des données et au risque de verrouillage technologique ressortent également des discours. Les analyses critiques des participants relatives à la privatisation de la sécurité et de la gouvernance algorithmique rejoignent les observations faites par Charlier et al. (2025).

Malgré l'utilité opérationnelle dévolue aux caméras augmentées, plusieurs participants expriment une volonté de ne pas verser vers une surveillance généralisée de l'espace public. Rigouste (2018) parle quant à lui de « panoptique policier » dénonçant également ce risque de surveillance généralisé (p. 41) pouvant même tendre, selon lui, jusqu'à une forme d'autocontrôle car « l'une des spécificités de l'ère sécuritaire est la recherche effrénée de la prise en charge du contrôle par les dominés eux-mêmes » (p. 45). Selon Lyon (2022), la surveillance ne se limite plus à l'observation ciblée de personnes suspectes mais concerne désormais l'ensemble de la population ses activités quotidiennes. Il souligne également que les technologies numériques, les bases de données et les dispositifs automatisés ont considérablement accru les capacités de collectes et d'analyse des données personnelles tant par les acteurs privés que par les acteurs publics. Dans le même sens, Zuboff (2022) dénonce une logique économique d'extraction massive de données comportementales par les grandes entreprises technologiques. Ces deux auteurs émettent de réelles préoccupations quant aux risques relatifs aux libertés individuelles, tels que le « social sorting » et la création d'un déséquilibre de pouvoir entre les institutions et les citoyens, engendrés par la surveillance et la collecte des données.

Les résultats montrent également des préoccupations marquées concernant la question des biais algorithmiques. Ces derniers peuvent être défini comme « une déviation par rapport à un résultat censé être neutre, loyal ou encore équitable ». Les questions qu'ils soulèvent « sont multiples et portent successivement sur la transparence, l'auditabilité, l'explicabilité, l'interprétabilité et la responsabilité des algorithmes » (Bertail et al., 2019, p. 7). Les algorithmes ont besoin de données pour produire des résultats. Par conséquent, la qualité des résultats dépend de la qualité des données. Dans la littérature, il est possible de trouver l'acronyme GIGO, venant de « Garbage in, garbage out ». Ce dernier fait référence au fait que l'algorithme produira des résultats inexacts ou potentiellement biaisés si ses données d'entrainement le sont-elles aussi (Bertail et al., 2019). Dès lors, si les systèmes apprennent à partir de données historiquement marquées par des pratiques policières ou des déséquilibres sociaux, le risque de discrimination indirecte augmente et peut contribuer à renforcer des inégalités déjà existantes, en particulier envers les populations précarisées et marginalisées (Eubanks, 2018, cité par Faith, 2019). En outre, les résultats des algorithmes dépendent également « de la manière dont les programmateurs les ont écrits » (Bertail et al., 2019, p. 9). Or ces derniers ne sont pas exempts de biais cognitifs, pouvant ainsi devenir des biais algorithmiques. Il existe aussi un risque de biais de variable omise (par exemple des compétences humaines compliquées à coder et à intégrer à l'algorithme) et des biais de sélection (apparaissant lorsque les caractéristiques de la population étudiée diffèrent de la population générale) (Bertail et al., 2019). Ainsi, « le défi de demain est de passer des « big data » aux « smart data » (Teller,

2024, p. 4). Puisque la qualité des données est un enjeu crucial, « elles doivent être équitables, « inclusives », c'est-à-dire représentatives des différentes tendances, et fiables dans le temps » (Teller, 2024, p. 4).

Pour pallier à certaines limites des technologies, la nécessité de maintenir l'humain au cœur du processus décisionnel a été soulignée à de multiples reprises par les participants. Cette position rejoint les exigences du Règlement Européen sur l'intelligence artificielle ainsi que le principe du « human in the loop » défendu dans la littérature éthique sur l'IA (Vuarin et al., 2023). Selon Vuarin et al. (2023), l'un des grands enjeux de l'IA responsable est d'éviter une automatisation totale des décisions. Pour rappel, les systèmes algorithmiques sont incapables de garantir une fiabilité totale (Kaenzig & Klauser, 2018, p. 63). De plus, ils peuvent développer des comportements trompeurs ou de produire des réponses orientées (Park et al., 2024). Puisque les décisions prises dans le contexte policier peuvent avoir d'importantes conséquences sur les libertés individuelles, la place de l'humain est nécessaire pour superviser les systèmes d'IA, valider les décisions, contrôler les résultats produits par les algorithmes et intervenir en cas de besoin. Toutefois, cette supervision humaine peut rester limitée ou symbolique lorsque les décisions des algorithmiques deviennent complexes ou que leur fonctionnement est opaque (Vuarin et al., 2023).

D'un côté, les dispositifs algorithmiques sont associés à une rationalisation du travail policier, un gain de temps et à une amélioration de l'efficacité opérationnel. De l'autre, il est associé à un risque de surcharge lié au traitement d'alertes, à la gestion des « faux positifs » et à la nécessité d'une supervision constante des systèmes. Cette ambivalence rejoint les analyses de Dupont (2004), pour qui les technologies produisent autant de contraintes organisationnelles qu'elles n'en résolvent. Par ailleurs, outre les contraintes organisationnelles et matérielles, l'impact environnemental des infrastructures numériques a été mis en lumière dans les résultats tout comme dans la littérature (Pachot & Patissier, 2022). L'IA dépend d'infrastructures matérielles (serveurs, des routeurs, disques durs) consommatrices de ressources énergétiques. Leur bon fonctionnement nécessite une consommation électrique continue. Cette activité permanente des infrastructures dégage de la chaleur. Il est donc nécessaire de mettre en place d'importants systèmes de refroidissement « qui constituent une source majeure de pollution » (TheGreenHhot, 2026, p. 4). A l'inverse, l'IA, dans certaines de ses applications, peut également contribuer à une réduction de la pollution. Par exemple, en permettant d'utiliser moins de pesticide ou en permettant une meilleure gestion de la circulation routière grâce aux caméras placées aux feux de circulation pour gérer l'alternance des feux de manière intelligente grâce à l'IA et ainsi minimiser de temps d'arrêts des véhicules (Pachot & Patissier, 2022).

Ainsi, l'intégration des caméras augmentées au sein des services de police est globalement perçue comme porteuse d'opportunités opérationnelles mais également de risques sur les plans démocratiques, éthique, organisationnel et environnemental.

Forces et limites de l'étude

Cette recherche présente plusieurs forces telles que la pertinence du sujet, particulièrement actuel dans une société contemporaine marquée par le développement croissant des technologies algorithmiques et des dispositifs caméras dans le domaine de la sécurité publique. L'approche qualitative a permis d'explorer de manière approfondie les perceptions, représentations et questionnements des participants concernant l'intégration et/ou l'utilisation de caméras augmentées par les forces de police. D'autant que la durée relativement longue des entretiens (de 1h00 à 2h40) a favorisé le développement de réponses nuancées et détaillées de la part des participants. Cette démarche permet également de compléter les apports théoriques de la littérature par une prise en compte des réalités de terrain et des contraintes

opérationnelles rencontrées par les acteurs concernés. Par ailleurs, la diversité des zones de police interrogées a permis de recueillir des points de vue variés selon les contextes organisationnels et les réalités locales.

Néanmoins, cette recherche n'est pas exempte de limites. La période écoulée entre le début des premiers entretiens et la finalisation du travail constitue une limite dans la mesure où les résultats peuvent ne plus refléter entièrement l'état actuel des pratiques et des perceptions (1er entretien réalisé le 09.04.25). Cette limite est d'autant plus importante que l'intégration des caméras augmentées s'inscrit dans une matière en constante évolution, tant sur le plan technologique que juridique. Les caméras associées aux algorithmes sont encore peu développées ou peu utilisées dans certaines zones de police, ce qui a parfois limité la capacité des participants à se projeter concrètement sur certains enjeux abordés. Le fait que le cadre juridique ne soit pas encore très actualisé par rapport à cette matière à également contribuer à la prudence des participants. En outre, cette recherche ne visait pas une analyse approfondie des aspects purement techniques de ces technologies, mais davantage l'étude des perceptions et des enjeux liés à leur utilisation. Le caractère qualitatif et le nombre limité de participants ne permettent dès lors pas une généralisation des résultats à l'ensemble des fonctionnaires de police ou des acteurs concernés. De plus, le fait que les participants interrogés occupaient exclusivement des fonctions dirigeantes au sein des zones de police peut constituer une limite de cette recherche. Cette caractéristique de l'échantillon a pu influencer certains discours et favoriser un biais de désirabilité sociale. Effectivement, les participants ont pu être amenés à formuler des réponses conformes aux attentes institutionnelles. Finalement, les technologies étudiées n'étant pas très répandues, nous observons une confusion chez certains participants entre les concepts de caméras biométriques et de caméras augmentées. Cette confusion a pu être renforcée par le fait qu'au début de notre étude, nous employions le terme de « vidéosurveillance algorithmique » pour désigner les dispositifs analysés. Ce n'est qu'après nos échanges avec les participants que nous avons revu notre choix terminologique. Nous avons ainsi privilégié l'expression « caméras augmentées » afin de nous aligner davantage à la terminologie juridique.

Perspectives futures

Ces constats ouvrent plusieurs pistes pour de futures recherches. Il pourrait être pertinent d'approfondir l'étude des collaborations entre les acteurs publics et privés dans l'intégration et l'utilisation des algorithmes aux systèmes des caméras, notamment au regard des enjeux de légitimité, de contrôle et de responsabilité. Des recherches quantitatives menées à plus grande échelle permettraient également de comparer les perceptions entre différentes zones de police. Au regard de la distinction théorique soulignée par les participants entre la police administrative et la police judiciaire, il pourrait être intéressant d'analyser, dans de futures recherches, l'intégration des technologies algorithmiques à l'échelle de l'ensemble de la police intégrée. Des approches comparatives entre différentes villes ou pays, que ce soit au niveau européen ou mondial, permettrait également d'apporter un éclairage complémentaire sur les pratiques et cadres d'utilisation de ces dispositifs. Enfin, des recherches futures pourraient examiner les perceptions des dispositifs technologiques auprès d'autres catégories d'acteurs tels que des citoyens, des décideurs politiques, des juristes, des ONG actives dans la protection des droits fondamentaux, etc.

6. Conclusion

Ce travail de fin d'études avait pour ambition d'analyser les perceptions des fonctionnaires dirigeants de police local belges sur les enjeux et défis de l'intégration, dans leurs pratiques de maintien de l'ordre public, des caméras couplées aux algorithmes. Nous questionnions notamment l'impact de ces technologies sur la sécurité publique et les droits fondamentaux des citoyens. Cette recherche à visée

exploratoire a été menée auprès de 12 participants par le biais d'entretiens semi-directifs. L'analyse des résultats met en exergue que l'intégration des caméras dites augmentées au sein des forces de police s'inscrit dans un cadre de gouvernance complexe, caractérisé par une multiplicité de normes juridiques, d'acteurs institutionnels et d'exigences relatives à la protection des données. Les participants soulignent l'importance d'un encadrement basé sur les principes du « privacy by design », de traçabilité, de transparence et de contrôle humain pour garantir la légitimité et l'acceptabilité de ces dispositifs algorithmiques.

Sur le plan opérationnel, les caméras augmentées sont principalement perçues comme des aides à la décision permettant d'améliorer la gestion de l'ordre public, de soutenir et de sécuriser les interventions policières. Elles permettent aussi une exploitation plus rapide et efficace des images dans le cadre des enquêtes judiciaires. Les caméras augmentées sont également associées à un gain de temps et d'efficacité organisationnelles grâce à l'automatisation de certaines tâches et à une meilleure gestion du flux d'informations. En revanche, leur potentiel préventif est considéré comme limité et dépendant du contexte dans lequel elles sont déployées.

Malgré un engouement pour l'intégration future de ces technologies, plusieurs défis liés à leur déploiement ont été soulevés. Les contraintes financières, infrastructurelles, environnementales et humaines constituent des obstacles importants. A ceux-ci s'ajoutent des risques liés à la qualité des données, aux faux positifs et à la surcharge générée par le traitement des alertes. Dans ce contexte, l'ensemble des participants insiste sur la nécessité de maintenir une supervision humaine permanente ainsi que sur le besoin de formations pour garantir un usage adéquat de ces outils par les utilisateurs.

Enfin, les résultats révèlent des préoccupations concernant les droits fondamentaux, notamment la protection de la vie privée, les risques de discrimination engendrés par les biais algorithmiques, la surveillance excessive et la sécurité des données. L'encadrement démocratique des dispositifs ainsi que la confiance accordée aux institutions semblent être des éléments déterminants pour l'acceptabilité sociale de l'intégration des caméras augmentées. Outre ces préoccupations, les résultats exposent également des enjeux de souveraineté numérique et des tensions liées à la dépendance envers les fournisseurs privés mettant en avant la nécessité de préserver le contrôle institutionnel sur les données, les infrastructures et les processus décisionnels.

En conclusion, les caméras augmentées sont globalement perçues comme des outils susceptibles d'améliorer l'efficacité des pratiques policières à condition qu'elles soient intégrées dans un cadre juridique, éthique et organisationnel rigoureux. Au vu du caractère exploratoire de cette recherche et du nombre limité de participants, les résultats ne visent pas à être généralisés. Ils ne reflètent effectivement pas l'ensemble des perceptions des fonctionnaires dirigeants de police locale. Néanmoins, ils permettent d'identifier des enjeux centraux et des pistes de réflexion susceptibles d'alimenter des débats scientifiques, politiques et opérationnels relatifs au recours à l'intelligence artificielle dans le domaine de la sécurité publique. De futures études pourraient par exemple s'intéresser aux collaborations public-privé. Des études quantitatives à plus grande échelle pourraient aussi comparer les perceptions entre zones de police tandis que d'autres travaux pourraient analyser l'intégration de ces technologies à l'échelle de l'ensemble de la police intégrée. Enfin, des approches comparatives et multi-acteurs permettraient de compléter l'éclairage sur les pratiques et les cadres d'usage.

Bibliographie

Ouvrages

Bouchard, S., & Cyr, C. (2005). Recherche psychosociale : pour harmoniser recherche et pratique (2e édition.). Presses de l'Université du Québec.

Foucault, M. (1975). *Surveiller et punir : Naissance de la prison*. Gallimard.

Ford, M. (2015). Rise of the robots : technology and the threat of a jobless future. *Choice Reviews Online*, 53(01), 53-0326. https://doi.org/10.5860/choice.192294

Lafrate, F. (2018). Intelligence artificielle et big data : naissance d'une nouvelle intelligence (Vol. 7). ISTE Group.

Pachot, A., & Patissier, C. (2022). Intelligence artificielle et environnement: alliance ou nuisance?: l'IA face aux défis écologiques d'aujourd'hui et de demain. Dunod.

Paillé, P. et Mucchielli, A. (2021). Chapitre 1. Choisir une approche d'analyse qualitative. L'analyse qualitative en sciences humaines et sociales (p. 13-36). Armand Colin. https://shs.cairn.info/l-analyse-qualitative-en-sciences-humaines--9782200624019-page-13?lang=fr

Paillé, P. et Mucchielli, A. (2021). Chapitre 12. L'analyse thématique. L'analyse qualitative en sciences humaines et sociales (p. 269-357). Armand Colin. https://shs.cairn.info/l-analyse-qualitative-en-sciences-humaines--9782200624019-page-269?lang=fr

Poullet, Y. (2021). *Le RGPD face aux défis de l'intelligence artificielle*. Éditions Larcier.

Contribution à un ouvrage collectif

Keynes, J. M. (2010). Economic Possibilities for Our Grandchildren. *Dans Palgrave Macmillan UK eBooks*. p. 321-332. https://doi.org/10.1007/978-1-349-59072-8_25

Pickover, C. (2021). La conférence de Dartmouth sur l'IA. La fabuleuse histoire de l'intelligence artificielle : Des automates aux robots humanoïdes. p. 140 -141. Dunod. https://stm.cairn.info/la-fabuleuse-histoire-de-l-intelligence-artificielle--9782100813186-page-140?lang=fr

Savoie-Zajc, L. (2007). Comment peut-on construire un échantillonnage scientifiquement valide ? Dans Recherche qualitative en sciences humaines et sociales : les questions de l'heure, p. 99-111. Association pour la recherche qualitative.

Articles de revue

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2477899

Berckmans, J. (2024). Vers une organisation de police numériquement transformée. *Dans Blue Minds*, 8(3), p. 3. Vanden Broele.

Besse, P., Castets-Renard, C., Garivier, A., & Loubes, J. M. (2018). *L'IA du quotidien peut-elle être éthique?* Statistique et Société, 6(3), p. 9-31.

Bocquet, N. (2021). La Smart City à Bruxelles : quand « intelligence » rime avec vidéosurveillance. *Brussels Studies*. https://doi.org/10.4000/brussels.5655

Bradford, B., Yesberg, J. A., Jackson, J., & Dawson, P. (2020). Live Facial Recognition : Trust and Legitimacy as Predictors of Public Support for Police Use of New Technology. The British Journal Of Criminology. https://doi.org/10.1093/bjc/azaa032

Bragias, A., Hine, K., & Fleet, R. (2021). "Only in our best interest, right ?" Public perceptions of police use of facial recognition technology. Police Practice And Research, 22(6), 1637-1654. https://doi.org/10.1080/15614263.2021.1942873

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research In Psychology, 3(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. Qualitative Research In Sport Exercise And Health, 11(4), 589-597. https://doi.org/10.1080/2159676x.2019.1628806

Bromberg, D. E., Charbonneau, É., & Smith, A. (2018). Body-Worn Cameras and Policing : A List Experiment of Citizen Overt and True Support. Public Administration Review, 78(6), 883-891. https://doi.org/10.1111/puar.12924

Charlier, R., Picaud, M., & Castagnino, F. (2025). From the "safe city" to digital urban security systems. *Réseaux*, N° 251(3), p. 11-43. https://doi.org/10.3917/res.251.0011

Campion, J. (2020). Stabilité et crises du système policier belge (1830-2018). Lien Social et Politiques, 84, 35-59. https://doi.org/10.7202/1069442ar

Cardon, D. (2018). *Le pouvoir des algorithmes. Pouvoirs, N° 164(1)*, p. 63-73. https://doi.org/10.3917/pouv.164.0063

Castets-Renard, C. (2018). Régulation des algorithmes et gouvernance du machine learning: vers une transparence et «explicabilité» des décisions algorithmiques?(Algorithm Regulation and Machine Learning Governance: Towards Transparency and'Explainability'of Algorithmic Decisions?). Revue Droit & Affaires, Revue Paris II Assas, 15ème édition.

Cavoukian, A. (2012). Privacy by Design [Leading Edge]. IEEE Technology And Society Magazine, 31(4), 18-19. https://doi.org/10.1109/mts.2012.2225459

Crawford, A. (2006). Networked governance and the post-regulatory state ? Theoretical Criminology, 10(4), 449-479. https://doi.org/10.1177/1362480606068874

Davies, A., & Krame, G. (2023). Integrating body-worn cameras, drones, and AI : A framework for enhancing police readiness and response. Policing A Journal Of Policy And Practice, 17. https://doi.org/10.1093/police/paad083

Debailleul, C. (2023). *Vidéosurveillance à Bruxelles: installer des caméras, mais pourquoi?* La chronique de la ligue des droits de l'homme, (203).

De Keersmaecker, P., & Debailleul, C. (2016). Répartition géographique de la vidéosurveillance dans les lieux publics de la Région de Bruxelles-Capitale. *Brussels Studies*. https://doi.org/10.4000/brussels.1422

Depussay, L. (2007). Hiérarchie des normes et hiérarchie des pouvoirs. Revue du droit public, Mars(2), p. 421-443. https://droit.cairn.info/revue-revue-du-droit-public-2007-2-page-421?lang=fr

Doberstein, C., Charbonneau, É., Morin, G., & Despatie, S. (2021). Measuring the Acceptability of Facial Recognition-Enabled Work Surveillance Cameras in the Public and Private Sector. *Public Performance & Management Review*, 45(1), 198-227. https://doi.org/10.1080/15309576.2021.1931374

Faith, G. (2019). *Virginia Eubanks (2018) Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. New York: Picador, St Martin's Press*. *Law, Technology and Humans, 1*(1), 162-164. https://doi.org/10.5204/lthj.v1i0.1386

Farzaneh, F., & Boyer, A. (2021). L'être humain face à l'IA : soumis ou dominant ? *Gestion 2000*, *Volume* 38(2), p. 157-179. https://doi.org/10.3917/g2000.382.0157

Faqir, R. (2023). Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview. International Journal of Cyber Criminology, vol. 17 (2), p. 77-94. DOI : 10.5281/zenodo.4766706

Feldstein, S. (2019). The Global Expansion of AI Surveillance. *Carnegie Endowment For International Peace*.https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en

Ferrari, M. V. (2022). Test, swarm, normalize : how surveillance technologies have infiltrated Paris 2024 Olympic Games. Cadernos Metrópole, 25(56), 75-96. https://doi.org/10.1590/2236-9996.2023-5603

Georges, B. (2019). Intelligence artificielle : de quoi parle-t-on ? *Constructif*, N° 54(3), p. 5-10. https://doi.org/10.3917/const.054.0005

Gesny, O. (2019). Capter l'IA de demain au regard des enjeux de cyberdéfense. *Revue Défense Nationale*, N° 820(5), 38-42. https://doi.org/10.3917/rdna.820.0038

Goodman, B., & Flaxman, S. (2017). European Union Regulations on Algorithmic Decision Making and a "Right to Explanation". *AI Magazine*, 38(3), 50-57. https://doi.org/10.1609/aimag.v38i3.2741

Hadjadji, N. & Blanc, O. (2024). Les angles morts de la vidéosurveillance algorithmique. Socialter, 62(2), 86-87. https://shs.cairn.info/magazine-socialter-2024-2-page-86?lang=fr

Haiech, J. (2020). Parcourir l'histoire de l'intelligence artificielle, pour mieux la définir et la comprendre. *Médecine/Sciences*, 36(10), 919-923. https://doi.org/10.1051/medsci/2020145

Heyman, V. (2024). La puissance de l'écoute active. Cahiers Pédagogiques, N° 590(1), 45-46. https://doi.org/10.3917/cape.590.0045

Hirose, M. (2017). Privacy in public spaces: The reasonable expectation of privacy against the dragnet use of facial recognition technology. Connecticut Law Review, 49(5), 1591–1620. https://opencommons.uconn.edu/law_review/377

Introna, L., & Nissenbaum, H. (2010). Facial Recognition Technology A Survey of Policy and Implementation Issues. SSRN Electronic Journal. https://eprints.lancs.ac.uk/id/eprint/49012

Javed, A., & Noman, S. (2012). AJ Theft Prevention Alarm Based Video Summarization Algorithm. *International Journal Of Information And Education Technology*, 23-28. https://doi.org/10.7763/ijiet.2012.v2.76

Kaenzig, R., & Klauser, F. (2018). Vidéosurveillance et insécurités urbaines : Etude de l'efficacité préventive du dispositif de caméras installé au quartier des Pâquis à Genève. Geographica Helvetica, 73(1), 63-73. https://doi.org/10.5194/gh-73-63-2018

Klarin, H. (2024). Regulation and Implementation of AI from a European Perspective: Opportunities, Risks, and Ethical Considerations. *Journal of Offender Monitoring*, *37*(1).

Kelsen, H. (2022). Dieu et l'État. *Droits*, *n° 73*(1), 169-186. https://doi.org/10.3917/droit.073.0169

Lacroux, A., & Martin-Lacroux, C. (2021). L'Intelligence artificielle au service de la lutte contre les discriminations dans le recrutement : nouvelles promesses et nouveaux risques. *Management & Avenir*, N° 122(2), p. 121-142. https://doi.org/10.3917/mav.122.0121

Laref, L., & Laref, M. (2025). De la surveillance des événements sportifs à la surveillance des Jeux Olympiques et Paralympiques de Paris 2024 : la sécurité triomphante ? Cultures & Conflits/Cultures et Conflits, 138, 65-83. https://doi.org/10.4000/14531

Lastrayoli, P. (2024). Vers une organisation de police numériquement transformée. *Dans Blue Minds*, 8(3), Vanden Broele.

Laurier, D. (2024). Vers une organisation de police numériquement transformée. *Dans Blue Minds, 8(3),* (p. 7). Vanden Broele.

Lemoigne, J. (2020). Intelligence artificielle et raisonnement économique. Mondes En Développement, n° 192(4), 189-190. https://doi.org/10.3917/med.192.0189

Le Pollotec, Y. (2018). Intelligence artificielle : le rapport de Cédric Villani. *La Pensée*, N° 396(4), p. 73-85. https://doi.org/10.3917/lp.396.0073

Lum, K., & Isaac, W. (2016). To Predict and Serve ? *Significance*, *13*(5), 14-19. https://doi.org/10.1111/j.1740-9713.2016.00960.x

Lunter, J. (2020). Beating the bias in facial recognition technology. Biometric Technology Today, 2020(9), 5-7. https://doi.org/10.1016/s0969-4765(20)30122-3

Lyon, D. (2022). Surveillance. Internet Policy Review, 11(4). https://doi.org/10.14763/2022.4.1673

Mateen, H. (2018). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. *Berkeley Journal Of Employment And Labor Law*, 39(1), 285. https://doi.org/10.15779/z388c9r431

Nouh, M., Nurse, J. R. C., Webb, H., & Goldsmith, M. (2019). Cybercrime Investigators are Users Too ! Understanding the Socio-Technical Challenges Faced by Law Enforcement. Kent Academic Repository (University Of Kent). https://doi.org/10.48550/arxiv.1902.06961

Nzobonimpa, S. (2022). L'utilisation des technologies d'apprentissage automatique par la police préoccupe-t-elle les intervenants québécois ? *Criminologie, 55(1*), 271. https://doi.org/10.7202/1089737ar

Park, P. S., Goldstein, S., O'Gara, A., Chen, M., & Hendrycks, D. (2024b). AI deception : A survey of examples, risks, and potential solutions. Patterns, 5(5), 100988. https://doi.org/10.1016/j.patter.2024.100988

Pasquale, F. (2016). The Black Box Society: The Secret Algorithms That Control Money and Information. *Contemporary Sociology A Journal Of Reviews*, 45(3), p. 367-368. https://doi.org/10.1177/0094306116641409c

Proulx, A. G., & Dionne, E. (2010). Blanchet, A., & ; Gotman, A. (2007). Série « L'enquête et ses méthodes » : L'entretien (2e éd. refondue). Paris : Armand Colin. Mesure et Évaluation En Éducation, 33(2), 127. https://doi.org/10.7202/1024898ar

Rigouste, M. (2018). La police du futur. Revue du Crieur, N° 10(2), p. 32-47. https://doi.org/10.3917/crieu.010.0032

Rondeau, K., Paillé, P., & Bédard, E. (2023). La confection d'un guide d'entretien pas à pas dans l'enquête qualitative. Recherches Qualitatives, 42(1), 5-29. https://doi.org/10.7202/1100242ar

Tallent, A. (2024). Le régime de surveillance olympique. *Esprit, Juillet-Août* (7), p. 16-19. https://doi.org/10.3917/espri.2407.0016

Teller, M. (2024). L'apport du droit dans la régulation de l'intelligence artificielle : penser la démocratie algorithmique. Journal Of Artificial Intelligence For Sustainable Development., 1(1). https://doi.org/10.69828/4d4knd

Trstenjak, M. (2024). Analyse des bacs à sable réglementaires d'IA dans l'AI Act. Pin Code, N° 19(3), p. 11-17. https://doi.org/10.3917/pinc.019.0011

Van Biervliet, D., Maesschalck, J., & Rooseleers, L. (2025). Technologie dans la police locale belge : La distribution (wallonne) en 2023. Revue de droit pénal et de criminologie, 3, p. 271–295.

Villani, C. (2019). Les enjeux de l'IA pour la Défense de demain. *Revue Défense Nationale*, N° 820(5), 23-29. https://doi.org/10.3917/rdna.820.0023

Vuarin, L., Lopes, P. G., & Massé, D. (2023). L'intelligence artificielle peut-elle être une innovation responsable ? Innovations, N° 72(3), 103-147. https://doi.org/10.3917/inno.pr2.0153

Wilson, J. Q., & Kelling, G. L. (1982). The Police and Neighborhood Safety:
Broken windows, Atlantic Monthly, vol. 3, n° 249, p. 29-38. https://media4.manhattan-institute.org/pdf/_atlantic_monthly-broken_windows.pdf

Wyvekens, A. (2008). Quand l'urbain rencontre la sécurité. La prévention situationnelle en France aujourd'hui. *Revue de droit pénal et de criminologie*, 2008, 9-10, pp.887-900.

Zatsepina, L., & Ludvigsen, J. A. L. (2025). Algorithmic Olympics : exploring the ethical and social implications of AI surveillance through the case of Paris 2024. International Journal Of Sport Policy And Politics, 17(3), 439-460. https://doi.org/10.1080/19406940.2025.2529201

Zuboff, S. (2022). Surveillance Capitalism or Democracy ? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization. Organization Theory, 3(3). https://doi.org/10.1177/26317877221129290

Littérature grise

Australian Institute of Criminology. (2003, June 17). *Understanding situational crime prevention* (AICrime Reduction Matters, No. 3, ISSN 1448-1383). https://www.aic.gov.au/sites/default/files/2020-05/crm003.pdf

Bertail, P., Bounie, D., Clémençon, S., & Waelbroeck, P. (2019). *Algorithmes : biais, discrimination et équit*é. Télécom ParisTech. https://www.telecom-paris.fr/wp-content-EvDsK19/uploads/2019/02/Algorithmes-Biais-discrimination-equite.pdf

Boudreau, C., Tremblay, M., & Comeau, P.-A. (collab.). (2005). L'utilisation des caméras de surveillance dans les lieux à accès public au Canada. École nationale d'administration publique (ÉNAP), Université du Québec.

Europol. (2024). AI and policing: The benefits and challenges of artificial intelligence for law enforcement. European Union Agency for Law Enforcement Cooperation.

Feldstein, S. (2019). The Global Expansion of AI Surveillance. *Carnegie Endowment For International Peace*.https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en

Fugier, P. (2010). Les approches compréhensives et cliniques des entretiens sociologiques. https://shs.hal.science/halshs-01651436v1

Fussey, P., & Murray, D. (2019). Independent report on the london metropolitan police service's trial of live facial recognition technology. University of Essex Human Rights Centre. https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf

Gakoue, A., & Gakoue, S. A. (2013). *La vidéosurveillance à l'Esplanade « Louvain-la-Neuve » : représentations des usagers*. https://hal.univ-lorraine.fr/hal-02334879.

Garvie, C., Bedoya, A. M., & Frankle, J. (2016). The perpetual line-up: Unregulated police face recognition in America. Georgetown Law Center on Privacy & Technology. https://www.perpetuallineup.org

Gill, M., & Spriggs, A. (2005). *Assessing the impact of CCTV*. Home office Research, Development and Satistics Directorate (research study 292). https://popcenter.asu.edu/sites/g/files/litvpz3631/files/Responses/video_surveillance/PDFs/Gill&Spriggs_2005.pdf

Larson, J., Mattu, S., Kirchner, L., & Angwin, J. (2016, May 23). *How we analyzed the COMPAS recidivism algorithm. ProPublica*. Retrieved from https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm

Trotta, M., & Donnay, J. (2017). Localisation des caméras ANPR sur le réseau routier pour le profilage géographique. hdl.handle.net. https://doi.org/10.3166/00047

Welsh, B.C., & Farrington, D.P. (2002). C*rime prevention effects of closed circuit television: A systematic review*. Home office Research, Development and Satistics Directorate (Research study 252). https://popcenter.asu.edu/sites/g/files/litvpz3631/files/Responses/video_surveillance/PDFs/Welsh&Farrington_2002.pdf

Police fédérale. (2011). *Typologie des zones de police : explications*. https://www.police.be/statistiques/sites/statspol/files/statistics_files_upload/VMS%20Archive/08_ELS-LVB%202011/01_ELS_2011_fr/04_Rapports%20typologie/typologie_zp_explications.pdf

Textes juridiques

Union européenne

Union européenne. (2016). *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données).* Journal officiel de l'Union européenne, L119, 1-88.

Union européenne. (2016). *Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention, d'enquete, de détection ou de poursuites d'infractions péneales ou d'éxécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision cadre 2008/977/ JAI du Conseil*. Journal officiel de l'Union européenne, L 119, 89-131. https://eur-lex.europa.eu/legal-

content/FR/TXT/?uri=CELEX%3A32016L0680&fbclid=IwY2xjawIxRgVleHRuA2FlbQIxMAABHUOX0IlHdpr7hSNrMEKaUjaMIAYCLjLbVuce7MNokQj3bgp2UYYUWr6d2Q_aem__1N6NskMoG51K8vGMo509A

Belgique

Belgique. (1994). La Constitution belge (Coordination officieuse du 17 février 1994). Sénat de Belgique. https://www.senate.be/doc/const_fr.html

Belgique. (2007). Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance. (2007). *Moniteur belge*, 31 mai 2007. https://www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=07-05-31&numac=2007000528

Belgique. (2018). Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. (2018). *Moniteur belge*, 5 septembre 2018. https://www.ejustice.just.fgov.be/cgi/article.pl?language=fr&sum_date=2026-04-07&pd_search=2018-09-05&numac_search=2018040581&page=1&lg_txt=F&caller=list&2018040581=0&view_numac=&numac=2018040581&choix1=et&choix2=et&fr=f&nl=n&du=d&trier=promulgation

Belgique. (2019). Loi du 22 mai 2019 modifiant diverses dispositions en ce qui concerne la gestion de l'information policière. (2019). Moniteur belge, 19 juin 2019. https://www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=19-06-19&numac=2019013125

Belgique. (2020). Loi du 8 juillet 2020 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras de surveillance par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière. (2018). *Moniteur belge*, 16 avril 2018. https://www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=20-07-15&numac=2020042286

Belgique. (2023). Loi du 19 octobre 2023 modifiant la loi du 5 août 1992 sur la fonction de police en ce qui concerne l'utilisation des caméras individuelles par les services de police. (2023). *Moniteur belge*, 20 novembre 2023.https://www.ejustice.just.fgov.be/cgi/article.pl?language=fr&sum_date=2026-04-07&pd_search=2023-11-20&numac_search=2023047049&page=1&lg_txt=F&caller=list&2023047049=0&view_numac=&numac=2023047049&choix1=et&choix2=et&fr=f&nl=n&du=d&trier=promulgation

Belgique. (2023). *Arrêté royal du 4 octobre 2023 portant création d'un Comité consultatif d'éthique des données et de l'intelligence artificielle de l'administration fédérale*. Moniteur belge. https://www.ejustice.just.fgov.be/eli/arrete/2023/10/04/2023045485/moniteur

Chambre des Représentants de Belgique. (2024). Proposition de loi insérant un nouvel article dans le Code d'instruction criminelle afin de mettre en œuvre l'article 5, paragraphe 5, du Règlement (UE) 2024/1689 sur l'intelligence artificielle (Doc. 56 0601/001). https://www.lachambre.be/flwb/pdf/56/0601/56K0601001.pdf

Documents officiels :

Belgique. (2025). Accord gouvernemental – Bart De Wever (2025-2029) [PDF]. https://www.belgium.be/sites/default/files/resources/publication/files/Accord_gouvernemental-Bart_De_Wever_fr.pdf

France

France. (2023). Loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions. *Journal officiel de la République française*. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047561974?__cf_chl_tk=3_J33ac9IBa8gcqmZlfzRhXIOfe2tmeuXg6sY5Zn4AA-1779443182-1.0.1.1-SnQ7DJz8TPNhTIymDLOxn_aymnXERs_hsPERMjg5wJQ.

Sites internet

Autorité de protection des données. (2025). *L'APD s'engage en faveur d'une IA innovante et respectueuse des données*. Consulté le 18 mars 2026 sur https://www.autoriteprotectiondonnees.be/citoyen/actualites/2025/09/18/l-apd-s-engage-en-faveur-d-une-ia-innovante-et-respectueuse-des-donnees

Autorité de protection des données. (*n.d.). Organisation.* Site de l'Autorité de protection des données. Consulté le 16 décembre 2024 sur https://www.autoriteprotectiondonnees.be/professionnel/l-autorite/organisation#:~:text=L'Autorité%20de%20protection%20des,des%20données%20à%20caractère%20personnel

BOSA. (*n.d.*). AI Act. Consulté de 11 février 2025 sur https://bosa.belgium.be/fr/themes/administration-numerique/strategie-et-politique-du-numerique/ai-act?fbclid=IwY2xjawIxZs5leHRuA2FlbQIxMAABHYT8BUgSoLMwimxGtpip55bSZ8J70PaQZrHB1yDn6pDDPyEXjtv2SUei8w_aem_OLiPbnZZq2Chy5UGvJxxYg

Centre de supervision Urbaine (CSU). *(n.d.*). Equans FR. https://www.equans-digital.com/centre-de-supervision-urbaine-csu

CNIL. (2025). *Joint Statement on Trustworthy Data Governance for AI : Twenty Data Protection Authorities Commit to Innovative and Privacy-Protecting AI*. Consulté le 18 mars 2026. https://www.cnil.fr/en/joint-statement-on-trustworthy-governance-for-ai-signed-by-twenty-dpa

Comité P. (*n.d.*). *Notre mission*. Consulté le 18 mars 2026 sur https://comitep.be/notre-mission.html

Démocratie.brussels. (*n.d.*). *Reconnaissance faciale dans la police*. Site de Démocratie.brussels. Consulté le 4 janvier 2025 sur https://democratie.brussels/initiatives/i-

155?locale=fr#:~:text=En%202017%20et%20en%202019,le%20logiciel%20controversé%20Clearview%20AI

Info, P. R. (2022, 5 novembre). Histoire belge : les caméras intelligentes qui vont sanctionner le GSM au volant sont. . . illégales. RTL Info. https://www.rtl.be/actu/belgique/societe/histoire-belge-les-cameras-intelligentes-qui-vont-sanctionner-le-gsm-au-volant/2022-11-05/article/499617

La Quadrature du Net. (2023, 15 mars). Les dangers de la vidéosurveillance algorithmique (VSA) [Vidéo]. YouTube. https://www.youtube.com/watch?v=DhXa3x-286Q

Metropolitan Police service. (2026). *Live facial recognition deployment record 2026*. Consulté le 04 avril 2026 sur https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/deployment-records/live-facial-recognition-deployment-record-2026.pdf

Metropolitan Police Service. (*n.d.). Facial recognition technology*. Consulté le 04 avril sur https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/facial-recognition-technology/

Ministère de l'Intérieur. (2025, 7 février). Expérimentation, en temps réel, de caméras « augmentées ». Consulté le 15 juin 2025 sur https://www.interieur.gouv.fr/actualites/actualites-du-ministere/experimentation-en-temps-reel-de-cameras-augmentees

Organe de contrôle de l'information policière. (*n.d*.). Section Home. Consulté le 06 avril 2026 sur https://www.organedecontrole.be

Parlement européen. (2020, 7 septembre). *Intelligence artificielle : définition et utilisation*. Site *du Parlement européen*. Consulté le 15 octobre 2024 sur https://www.europarl.europa.eu/topics/fr/article/20200827STO85804/intelligence-artificielle-definition-et-utilisation

Parlement européen. (2020, 18 septembre). *Intelligence artificielle : opportunités et risques. Site du Parlement européen.* Consulté le 30 décembre 2024 sur https://www.europarl.europa.eu/topics/fr/article/20200918STO87404/intelligence-artificielle-opportunites-et-risques

Police Locale Gaume. (*n.d*.). *L'usage de drones à la police de Gaume : présentation*. Consulté le 15 octobre 2024 sur https://www.police.be/5299/questions/usage-de-cameras-par-la-zone-de-police/lusage-de-drones-a-la-police-de-gaume-presentation

Police Locale Uccle / W-B / Auderghem. (*n. d*.). *Des bodycams pour filmer les interventions policières*. Consulté le 15 octobre 2024 sur https://www.police.be/5342/fr/questions/bodycam/des-bodycams-pour-filmer-les-interventions-policieres

Police Locale Uccle / W-B / Auderghem. (*n. d*.). Police Locale Uccle / W-B / Auderghem. Bodycam - questions fréquentes. Consulté le 11 février 2025 sur https://www.police.be/5342/fr/questions/bodycam/bodycam-questions-frequentes#:~:text=L'article%2025%2F3%20de,le%20cadre%20de%20leurs%20fonctions.

TheGreenShot. (2026, 21 janvier). Data centers : l&rsquo ; Impact réel sur l&rsquo ; environnement en 2025 (Chiffres Exclusifs). TheGreenShot. https://www.thegreenshot.io/fr/non-classe-fr/pollution-data-center/

Thèses / Mémoires

Mohamed kane, O. (2024). Intelligence artificielle et au-delà [Mémoire, Université du Québec à Trois-rivières]. https://depot-e.uqtr.ca/id/eprint/11312/

Verly, I. (2025). La bodycam dans la police belge : quels impacts sur les pratiques professionnelles ? (Mémoire de master, Université catholique de Louvain). https://thesis.dial.uclouvain.be/server/api/core/bitstreams/2f52e658-0346-4545-b3c1-f866ee44ce0c/content

Notes de cours

André, S. (2020-2021). Méthodologie de la recherche qualitative en criminologie [Notes de cours non publiées]. Université de Liège.

Annexes

Annexe 1 : Tableau récapitulatif des participants

Numéro du participant	Sexe (H/F/X)	Statut	Typologie de la zone de police
Participant 1	H	Commissaire divisionnaire (Service appui stratégique)	2
Participant 2	H	Commissaire de police (Service développement des applications)	1
Participant 3	F	Commissaire de police (Direction dispatching vidéo)	2
Participant 4	H	Direction stratégie organisationnelle et contrôle au niveau DPO)	4
Participant 5	H	DPO	1
Participant 6	H	Commissaire de police (Chef de service Centre Local de Communications/CCTV/Planification d'urgence)	1
Participant 7 et accompagnant	H et F	Direction de la stratégie et de l'audit et DPO	1
Participant 8	H	Consultant ICT – department research and development	2
Participant 9	H	Chef de corps	5
Participant 10	H	Chef de corps	4
Participant 11	H	Commissaire de police (Direction de l'Optimisation)	3
Participant 12	H	Commissaire Divisionnaire (Chef de corps)	3

Annexe 2 : Guide d'entretien semi-directif

Introduction générale sur la sécurité et les outils utilisés :

- Pouvez-vous vous présenter, me parler brièvement de votre formation, votre parcours professionnel dans la police et le cas échéant en dehors de la police ?

- Quel est et de votre rôle au sein de votre zone de police locale ?

- Quelles sont les principales missions et particularités (comme l'encadrement des manifestations sportives, culturelles ...) de votre zone de police en matière de maintien de l'ordre public et de sécurité ?

- Quels types d'outils (comme par exemple des chevaux de frise, barrières nadars, autopompe, …) utilisez-vous actuellement pour assurer la sécurité publique et le maintien de l'ordre ?

- Parmi ces outils, lesquels sont les plus efficaces selon vous ? Pourquoi ?

Introduction progressive à la vidéosurveillance :

- Votre zone de police utilise-t-elle la vidéosurveillance ? Si oui, depuis quand et dans quel cadre ? Quelles sont les facteurs qui ont entrainé la mise en place de ces caméras ?

- Comment ces systèmes sont-ils intégrés dans votre travail quotidien ? Qui les exploite et comment ?

- Quels sont, selon vous, les avantages et limites de la vidéosurveillance classique dans le cadre du maintien de l'ordre public ?

- Avez-vous constaté un impact de la vidéosurveillance sur la sécurité objective, autrement dit, avez-vous constaté une diminution de la délinquance grâce à ces systèmes ?

- Avez-vous constaté un impact de la vidéosurveillance sur la sécurité subjective, soit une diminution du sentiment d'insécurité ?

Introduction à l'intelligence artificielle en général :

- Connaissez-vous des exemples d'outils basés sur l'intelligence artificielle utilisés dans le domaine de la sécurité ou du maintien de l'ordre ? **Au besoin** : comme par exemple des caméras intelligentes, de l'analyse prédictive, drones intelligents, …)

- Votre zone de police locale utilise-t-elle certains de ces outils ? Si oui, lesquels ?

- Selon vous, quels sont les objectifs principaux de l'usage de ces outils ? (Prévention, dissuasion, gestion des foules, identification de suspects, ...)

- De manière générale, que pensez-vous de l'intégration de l'intelligence artificielle dans les pratiques policières ? Pourquoi ?

- Selon vous, dans quels domaines l'IA pourrait-elle être la plus utile pour la police locale ?

Passage à la vidéosurveillance algorithmique (VSA) :

- Avez-vous déjà entendu parler de la vidéosurveillance algorithmique (VSA) ? Si oui, quelles sont vos connaissances sur son fonctionnement et ses applications ?

- Avez -vous connaissance d'exemples dans lesquels cette technologie a été testée et a été particulièrement utile ou, au contraire, inefficace ?

- A votre connaissance, votre zone de police a-t-elle déjà testé ou envisagé d'utiliser des systèmes de vidéosurveillance basés sur l'IA ?

- Pouvez-vous me donner des exemples concrets d'utilisation de la vidéosurveillance algorithmique qui, selon vous, pourraient aider à mieux prévenir ou gérer des problèmes de sécurité ?

- Comment percevez-vous, personnellement, l'intégration des technologies de vidéosurveillance algorithmique dans le travail quotidien des forces de l'ordre ?

- Quels pourraient être les risques et défis liés à l'usage de la VSA dans la police locale ? (Fiabilité, biais, protection des données, acceptabilité citoyenne, etc)

- Quels pourraient être les principaux objectifs de l'utilisation de la VSA par la police locale ?

Cadre juridique et éthique :

- Avez-vous connaissance du cadre juridique encadrant les pratiques liées à ces technologies ? Avez-vous connaissance de ce qu'est L'IA Act ?

- Comment percevez-vous le cadre législatif actuel encadrant l'usage de ces technologies ? Est-il, selon vous, adapté aux réalités de terrain ? Quelles modifications pourraient éventuellement être mises en place ?

- Quelles sont les règles et protocoles qu'il faudrait, selon vous, mettre en place pour encadrer l'utilisation des systèmes algorithmiques par les zones de police locale ?

- Dans quelle mesure pensez-vous que la vidéosurveillance algorithmique peut poser des questions en matière de respect des droits fondamentaux ?

- Recevez-vous des retours de la population concernant l'utilisation de ces outils ? Si oui, lesquels sont-ils ?

- Pensez-vous qu'il est possible de construire un système de vidéosurveillance algorithmique éthique et protecteur de la vie privée ? Si non pourquoi et si oui comment faudrait-il s'y prendre selon vous ?

- Existe-il des formations spécifiques pour les agents afin de garantir un usage approprié de ces outils ?

Implication du secteur privé :

- A votre connaissance, la vidéosurveillance algorithmique implique-t-elle des collaborations avec des entreprises privées ? Si oui de quel type ?

- Comment se passe cette collaboration et quels en sont les enjeux ?

- Selon vous, jusqu'où l'implication du secteur privé est-elle acceptable dans la vidéosurveillance algorithmique ?

Perspectives et avis personnels :

- Selon vous, le recours à la vidéosurveillance algorithmique est-il opportun ? Si oui, doit-il être étendu et dans quel contexte ? Et si non, pourquoi ?

- Si vous pouviez formuler des recommandations sur l'usage de ces technologies par la police, lesquelles seraient-elles ?

Conclusion :

- Y a-t-il un aspect que nous n'avons pas abordé et que vous jugez important de mentionner ?

- Avez-vous des questions ?

Recrutement de participants suivants

+ Explication de la méthode « en boule de neige » et demande si autre participant à recommander.

Annexe 3 : Formulaire de consentement

Formulaire d'information et de consentement RGPD
pour un travail de fin d'étude

Travail de fin d'étude sur l'utilisation de la vidéosurveillance algorithmique par les forces de polices locales belges

Ce formulaire d'information et de consentement RGPD présente une description de l'étude et des traitements de données à caractère personnel qui y sont associés.

Nous vous demandons de lire attentivement ce document. Si vous êtes d'accord de prendre part à cette étude, vous devrez signer ce document. Une copie datée de ce document vous sera remise. Après avoir donné votre consentement à participer, vous resterez libre de vous retirer de cette étude à tout moment, sans qu'aucune justification ne soit nécessaire.

Si vous avez d'autres questions ou préoccupations concernant le projet ou vos données à caractère personnel, ou si vous souhaitez retirer votre participation, vous êtes libre de contacter le ou les responsables du projet de recherche à tout moment au moyen des coordonnées figurant ci-dessous.

Responsable(s) du projet de recherche

Le promoteur de ce travail de fin d'étude est : Monsieur Vincent Seron, chargé de cours à l'Université de Liège : vseron@uliege.be

L'étudiant réalisant ce travail de fin d'étude est : Chavée Chloé, étudiante en master de criminologie : Chloe.Chavee@student.uliege.be

Description de l'étude

Cette étude a pour but d'explorer les avantages et les inconvénients de l'utilisation de la vidéosurveillance algorithmique par les fonctionnaires de police locales pour le maintien de l'ordre public. Je m'interroge également sur la façon dont ces technologies pourraient potentiellement impacter la sécurité publique et les droits fondamentaux. Il s'agit d'une étude qualitative où des entretiens semi-directifs seront mener afin de récolter mes données. La durée de ces derniers sera comprise entre une et deux heures. Les entretiens se tiendront en présentiel au sein des zones de police concernées ou en distanciel selon les préférences du participant. Cette étude sera menée, sauf prolongation, jusqu'à la fin de l'année académique 2025.

Protection des données à caractère personnel

Le ou les responsables du projet prendront toutes les mesures nécessaires pour protéger la confidentialité et la sécurité de vos données à caractère personnel, conformément au *Règlement général sur la protection des données* (RGPD – UE 2016/679) et à la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

Qui est le responsable du traitement ?

Le Responsable du Traitement est l'Université de Liège, dont le siège est établi Place du 20-Août, 7, B-4000 Liège, Belgique.

Quelles seront les données collectées ?

Les données récoltées sont :

Des informations générales sur votre fonction, votre expérience et, si pertinent, certaines caractéristiques sociodémographiques (âge, sexe, lieu d'exercice).

Le contenu de vos réponses sur votre perception, vos expériences et vos opinions concernant l'usage de la vidéosurveillance algorithmique et son cadre légal et éthique.

Enregistrements audio des entretiens (avec votre accord) et transcriptions anonymisées.

À quelle(s) fin(s) ces données seront-elles récoltées ?

Les données à caractère personnel récoltées dans le cadre de cette étude serviront à la réalisation du travail de fin d'étude présenté ci-dessus. Elles pourraient, éventuellement, aussi servir à la publication de ce travail de fin d'étude ou d'articles issus de cette recherche, à la présentation de conférences ou de cours en lien avec cette recherche, et à la réalisation de toute activité permettant la diffusion des résultats scientifique de cette recherche. Votre anonymat sera garanti dans les résultats et lors de toute activité de diffusion de ceux-ci.

Combien de temps et par qui ces données seront-elles conservées ?

Les données à caractère personnel récoltées seront conservées jusqu'à la réalisation et la validation par le jury du travail de fin d'étude présenté ci-dessus. Le cas échéant, la conservation de ces données pourrait être allongée de quelques mois afin de permettre les autres finalités exposées au point 3.
Ces données seront exclusivement conservées par l'étudiant réalisant ce travail de fin d'étude, sous la direction de son promoteur.

Comment les données seront-elles collectées et protégées durant l'étude ?

Étape 1 : récolte des données lors d'entretiens individuels. Les données de contact et les réponses aux questions sont placées dans deux fichiers distincts. Il s'agira dans ce travail d'une pseudonymisation. Par conséquent, les réponses seront reliées aux données de contact via un code. Conservation des fichiers uniquement sur un disque dur protégé.
Étape 2 : traitement des réponses : comme les données de contacts ne sont plus nécessaires, suppression du fichier contenant ces données de contact. Les réponses deviennent donc purement anonymes.
Étape 3 : rédaction du TFE au moyen des réponses désormais anonymes.

Ces données seront-elles rendues anonymes ou pseudo-anonymes ?

Dans cette recherche, les données seront rendues pseudo-anonymes. Pseudonymisation signifie que les données ne seront plus liées à un nom et un prénom mais bien à un code, que seuls l'étudiant et son promoteur peuvent relier à des identités. La table de correspondance est conservée séparément jusque la fin de l'année académique (remise du travail).

Qui pourra consulter et utiliser ces données ?

Seuls l'étudiant réalisant le travail de fin d'étude présenté plus haut, son promoteur et éventuellement les membres du jury de mémoire (pour validation de la démarche scientifique) auront accès à ces données à caractère personnel.

Ces données seront-elles transférées hors de l'Université ?

Non, ces données ne feront l'objet d'aucun transfert ni traitement auprès de tiers.

Sur quelle base légale ces données seront-elles récoltées et traitées ?

La collecte et l'utilisation de vos données à caractère personnel se fondent sur la mission d'intérêt public de l'Université (RGPD, Art. 6.1.e) et, pour les données particulières, sur la nécessité de traiter ces données à des fins de recherche scientifique (RGPD, Art. 9.2.j).

Quels sont les droits dont dispose la personne dont les données sont utilisées ?

Comme le prévoit le RGPD (Art. 15 à 23), chaque personne concernée par le traitement de données peut, en justifiant de son identité, exercer une série de droits :
obtenir, sans frais, une copie des données à caractère personnel la concernant faisant l'objet d'un traitement dans le cadre de la présente étude et, le cas échéant, toute information disponible sur leur finalité, leur origine et leur destination;
obtenir, sans frais, la rectification de toute donnée à caractère personnel inexacte la concernant ainsi que d'obtenir que les données incomplètes soient complétées ;
obtenir, sous réserve des conditions prévues par la réglementation et sans frais, l'effacement de données à caractère personnel la concernant;
obtenir, sous réserve des conditions prévues par la réglementation et sans frais, la limitation du traitement de données à caractère personnel la concernant;
s'opposer, sous réserve des conditions prévues par la réglementation et sans frais, pour des raisons tenant à sa situation particulière, au traitement des données à caractère personnel la concernant ;
introduire une réclamation auprès de l'Autorité de protection des données (https://www.autoriteprotectiondonnees.be, contact@apd-gba.be).

Comment exercer ces droits ?

Pour exercer ces droits, vous pouvez vous adresser au Délégué à la protection des données de l'Université, soit par courrier électronique (dpo@uliege.be), soit par lettre datée et signée à l'adresse suivante :

Université de Liège
M. le Délégué à la protection des données,
Bât. B9 Cellule "GDPR",
Quartier Village 3,
Boulevard de Colonster 2,
4000 Liège, Belgique.

Coûts, rémunération et dédommagements

Aucun frais direct lié à votre participation à l'étude ne peut vous être imputé. De même, aucune rémunération ou compensation financière, sous quelle que forme que ce soit, ne vous sera octroyée en échange de votre participation à cette étude.

Retrait du consentement à participer à l'étude

Si vous souhaitez mettre un terme à votre participation à ce projet de recherche, veuillez en informer l'étudiant réalisant ce travail de fin d'étude et/ou son Promoteur, dont les noms figurent sur la première

page de ce document. Ce retrait peut se faire à tout moment, sans qu'une justification ne doive être fournie. Sachez néanmoins que les traitements déjà réalisés sur la base de vos données personnelles ne seront pas remis en cause. Par ailleurs, les données déjà collectées ne seront pas effacées si cette suppression rendait impossible ou entravait sérieusement la réalisation du projet de recherche. Vous en seriez alors averti.

Questions sur le projet de recherche

Toutes les questions relatives à cette recherche peuvent être adressées à l'étudiant réalisant le travail de fin d'étude, dont les coordonnées sont reprises ci-dessus.
Je déclare avoir lu et compris les 61 pages de ce présent formulaire et j'en ai reçu un exemplaire signé par les personnes responsables du projet. Je comprends la nature et le motif de ma participation au projet et ai eu l'occasion de poser des questions auxquelles j'ai reçu une réponse satisfaisante. Par la présente, j'accepte librement de participer au projet.

Nom et prénom :
Date :
Signature :

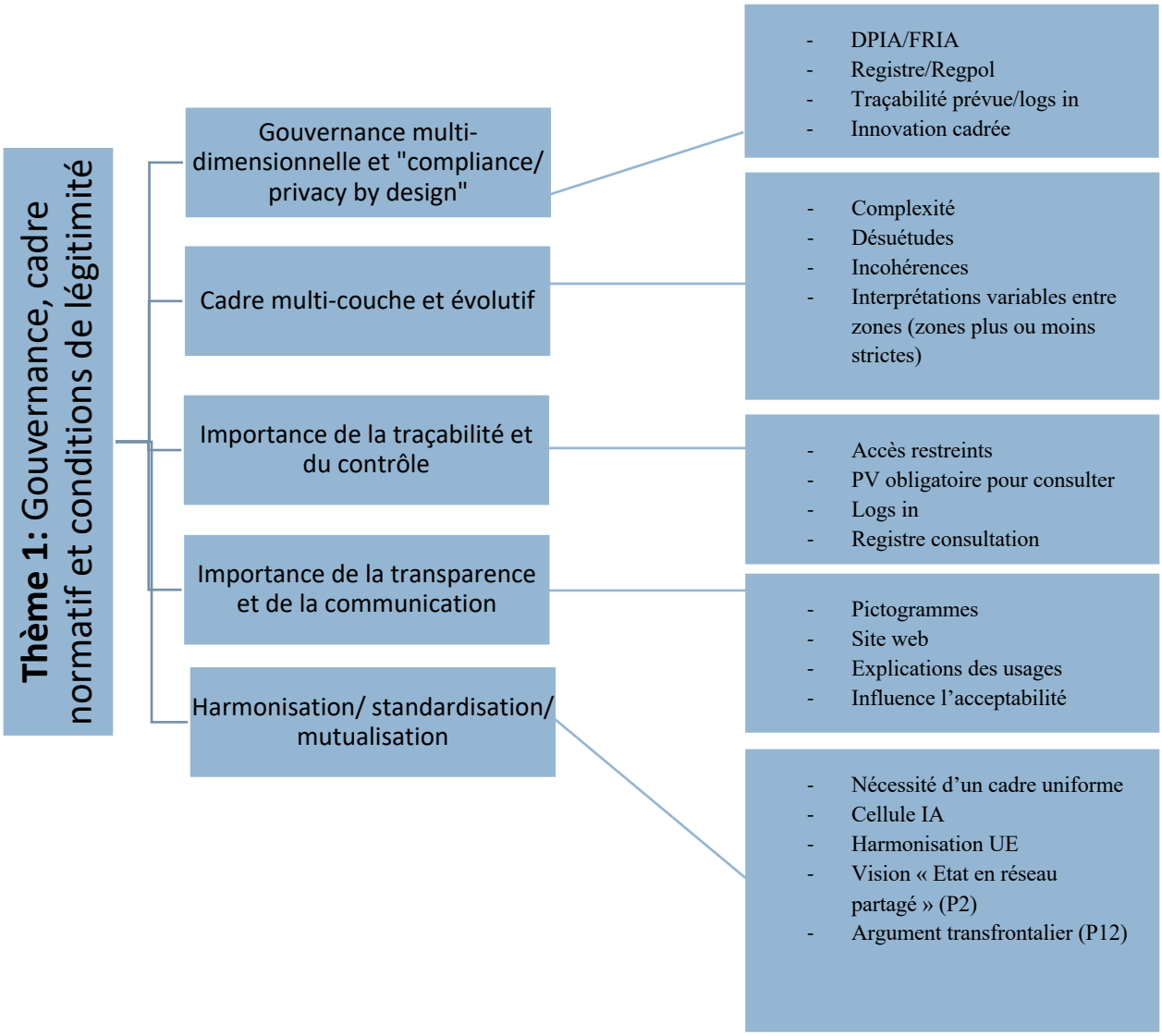
Nous déclarons être responsables du déroulement du présent projet de recherche. Nous nous engageons à respecter les obligations énoncées dans ce document et également à vous informer de tout élément qui serait susceptible de modifier la nature de votre consentement.

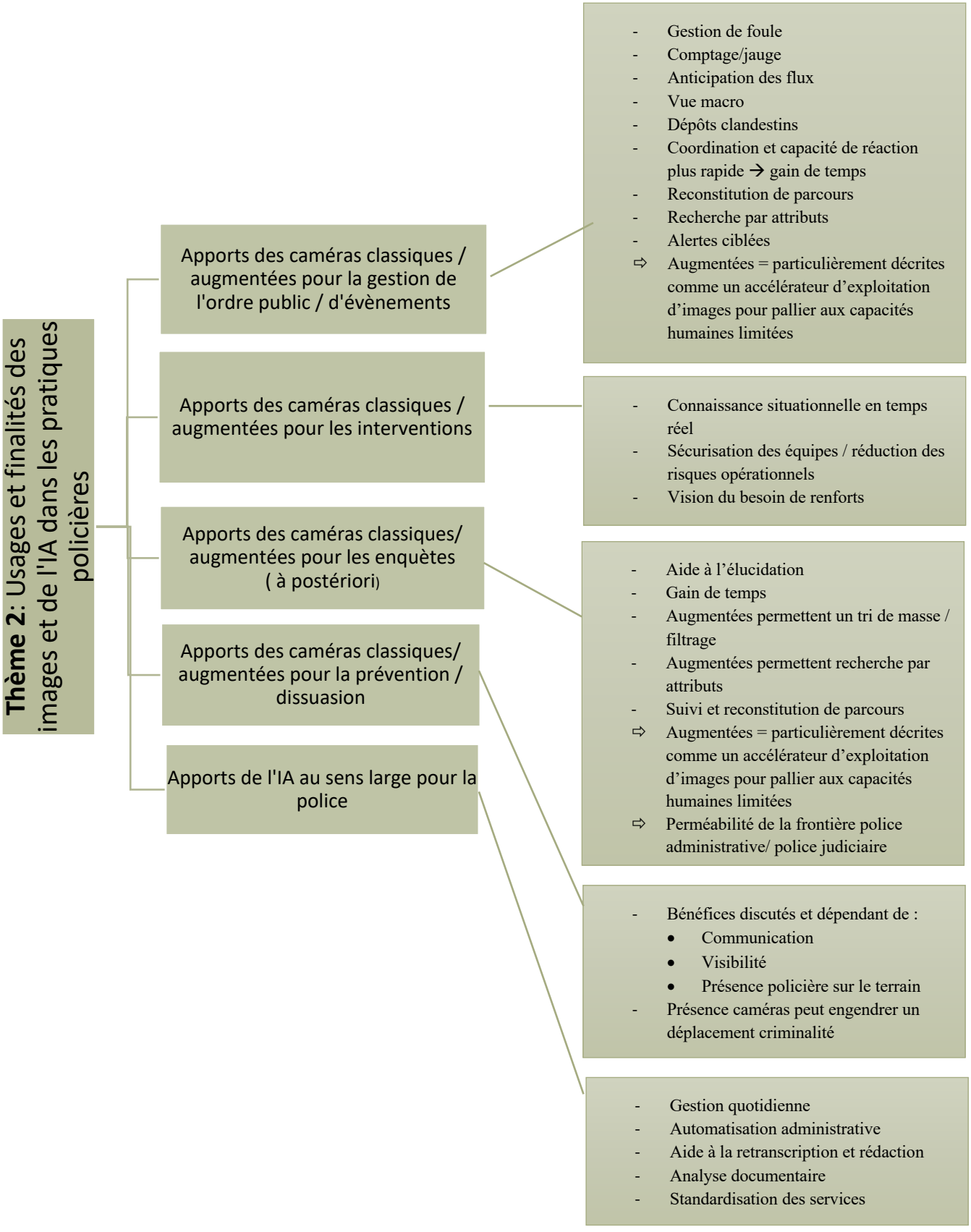
Nom et prénom du Promoteur :
Date :
Signature :

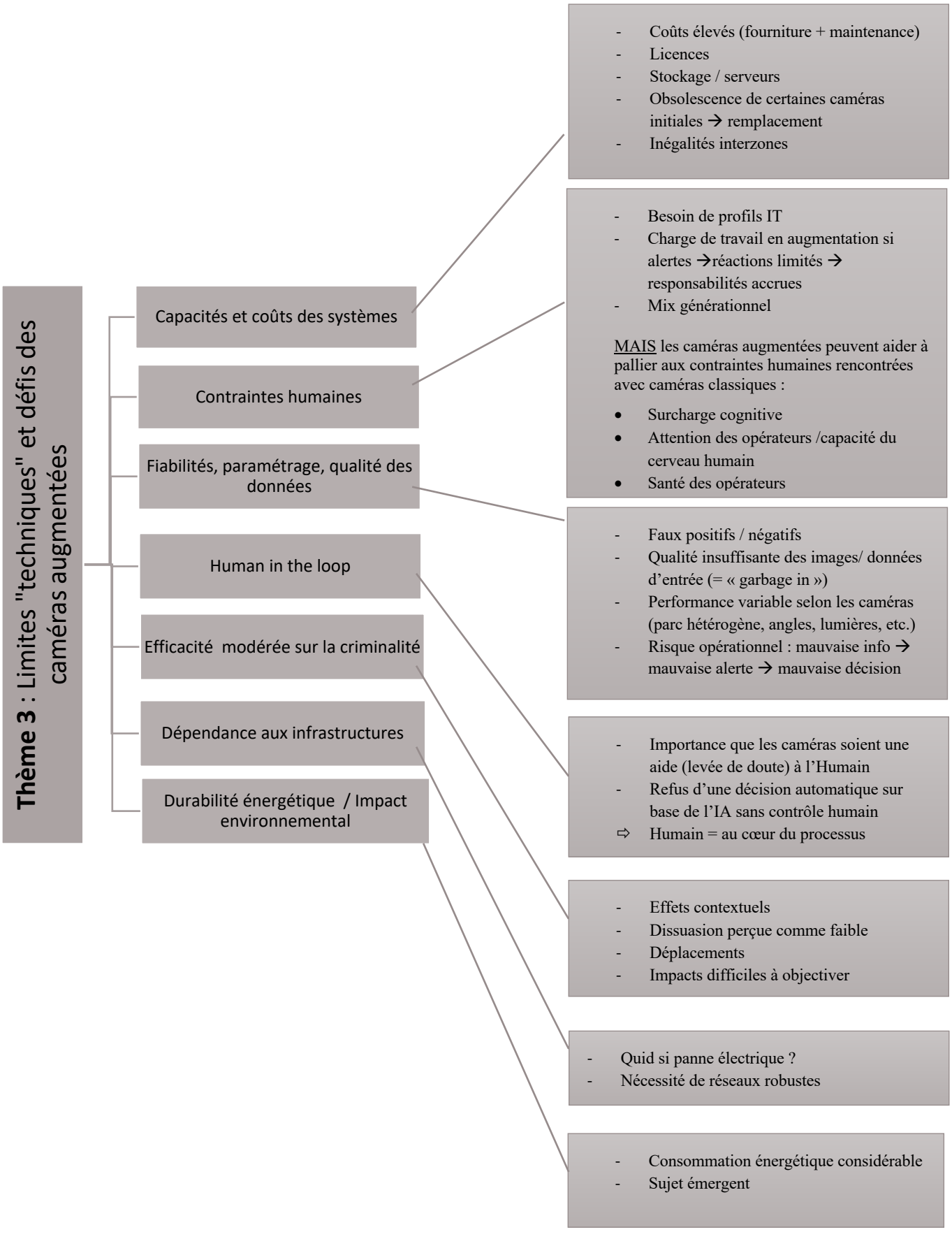
Nom et prénom de l'étudiant réalisant le travail de fin d'étude :
Date :
Signature :

Annexe 4 : Arbre thématique

Arbre thématique : 4 thèmes principaux




Thème 2: Usages et finalités des images et de l'IA dans les pratiques policières
Apports des caméras classiques / augmentées pour la gestion de l'ordre public / d'évènements
- Gestion de foule
- Comptage/jauge
- Anticipation des flux
- Vue macro
- Dépôts clandestins
- Coordination et capacité de réaction plus rapide → gain de temps
- Reconstitution de parcours
- Recherche par attributs
- Alertes ciblées
⇨ Augmentées = particulièrement décrites comme un accélérateur d'exploitation d'images pour pallier aux capacités humaines limitées
Apports des caméras classiques / augmentées pour les interventions
- Connaissance situationnelle en temps réel
- Sécurisation des équipes / réduction des risques opérationnels
- Vision du besoin de renforts
Apports des caméras classiques/ augmentées pour les enquêtes (à postériori)
- Aide à l'élucidation
- Gain de temps
- Augmentées permettent un tri de masse / filtrage
- Augmentées permettent recherche par attributs
- Suivi et reconstitution de parcours
⇨ Augmentées = particulièrement décrites comme un accélérateur d'exploitation d'images pour pallier aux capacités humaines limitées
⇨ Perméabilité de la frontière police administrative/ police judiciaire
Apports des caméras classiques/ augmentées pour la prévention / dissuasion
- Bénéfices discutés et dépendant de :
• Communication
• Visibilité
• Présence policière sur le terrain
- Présence caméras peut engendrer un déplacement criminalité
Apports de l'IA au sens large pour la police
- Gestion quotidienne
- Automatisation administrative
- Aide à la retranscription et rédaction
- Analyse documentaire
- Standardisation des services


Thème 3 : Limites "techniques" et défis des caméras augmentées
Capacités et coûts des systèmes
Contraintes humaines
Fiabilités, paramétrage, qualité des données
Human in the loop
Efficacité modérée sur la criminalité
Dépendance aux infrastructures
Durabilité énergétique / Impact environnemental
- Coûts élevés (fourniture + maintenance)
- Licences
- Stockage / serveurs
- Obsolescence de certaines caméras initiales → remplacement
- Inégalités interzones
- Besoin de profils IT
- Charge de travail en augmentation si alertes →réactions limités → responsabilités accrues
- Mix générationnel
MAIS les caméras augmentées peuvent aider à pallier aux contraintes humaines rencontrées avec caméras classiques :
• Surcharge cognitive
• Attention des opérateurs /capacité du cerveau humain
• Santé des opérateurs
- Faux positifs / négatifs
- Qualité insuffisante des images/ données d'entrée (= « garbage in »)
- Performance variable selon les caméras (parc hétérogène, angles, lumières, etc.)
- Risque opérationnel : mauvaise info → mauvaise alerte → mauvaise décision
- Importance que les caméras soient une aide (levée de doute) à l'Humain
- Refus d'une décision automatique sur base de l'IA sans contrôle humain
⇨ Humain = au cœur du processus
- Effets contextuels
- Dissuasion perçue comme faible
- Déplacements
- Impacts difficiles à objectiver
- Quid si panne électrique ?
- Nécessité de réseaux robustes
- Consommation énergétique considérable
- Sujet émergent

Thème 4 : Droits fondamentaux, risques de dérives et rapports de pouvoirs

Risques pour les droits fondamentaux

- Fuite des données / piratage
- Secret professionnel / instruction
- Respect vie privée
- Abus internes (ex : curiosité)
- Détournement des images
- Biais données d'entrainement → biais structurels (sur policing) → discriminations indirectes sur des critères apparemment neutre (effet de proxy)

Usages jugés innaceptables / disproportionnés

- Surveillance généralisée dans espace public
- Centralisation et croisement massif des données → traçabilité absolue / ranking social
- Prédiction des comportements

Point de bascule nécessitant un encadrement renforcé

- Biométrie / reconnaissance faciale → accepté et/ou souhaitée pour certains faits sous certaines conditions (ex : attentas)

Acceptabilité sociale et légitimité politique

- Débat de société / Parlementaire
- Polarisation
- Curseur mouvant (ex : terrorisme)
- Effets d'annonce
- Direction politique

Secteur privé, souveraineté et conditions d'accès

- Dépendance au secteur privé pour fourniture et maintenance

Mais, importance que police garde la maitrise des systèmes et des données :

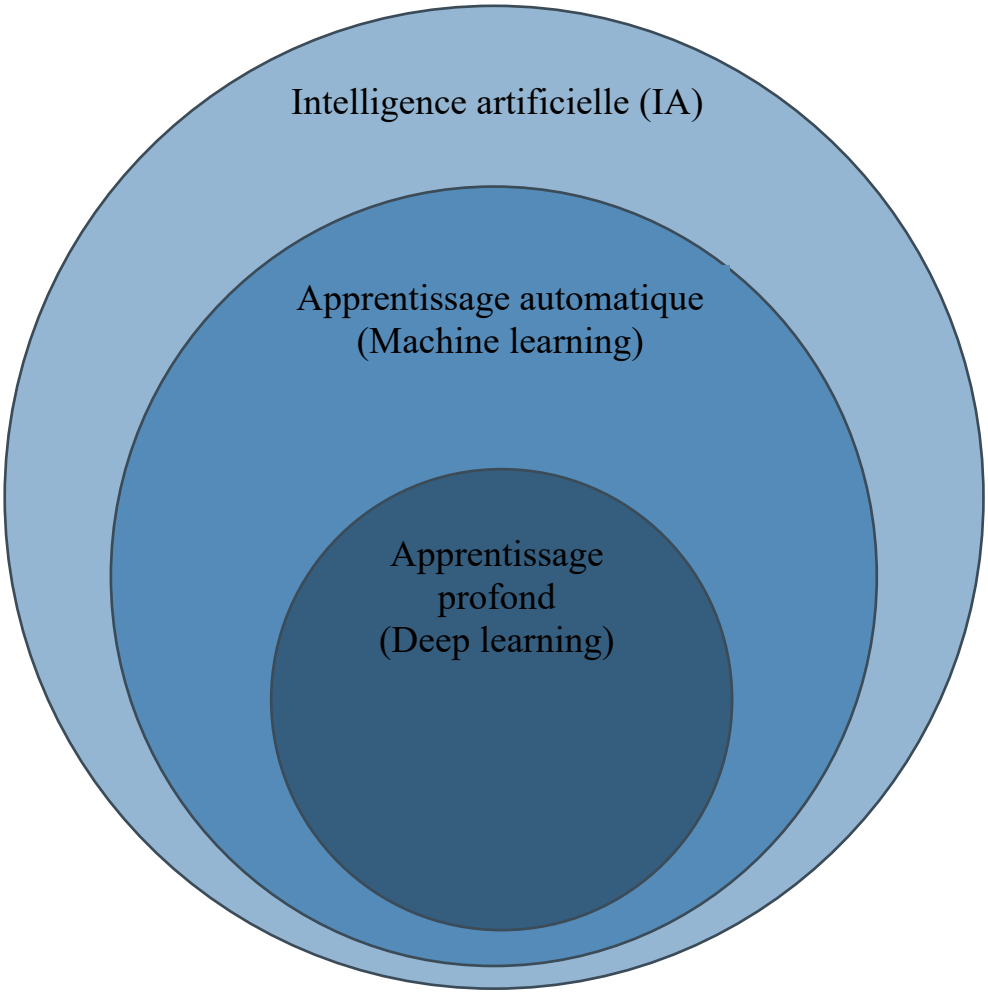
- Hébergement / serveurs police
- Accès / logs
- Refus cloud hors UE
- Refus d'une opacité totale du fonctionnement des systèmes (compréhension du paramétrage)
- Importance de disposer des compétences en interne
- Réduction de la dépendance à un fournisseur unique (Lock in)

Car :

- Crainte d'exfiltration
- Crainte d'une réutilisation des données par les fournisseurs
- Risque de monopole d'une société
- Quid si faillite ?
- Asymétrie commercial – technique

Donc :

- Clauses contractuelles (obligation de sécurité)
- Screening des fournisseurs

- Divergence quant à l'acceptabilité du visionnage des images par le privé : refus ou ouverture conditionnelle (sous règles/ contrôle/ responsabilité de la police)

Annexe 5 : Schéma représentant les relations hiérarchiques entre l'intelligence artificielle, l'apprentissage automatique et l'apprentissage profond