# Surveillance algorithmique des corps et des visages : une année 2024 décisive ?

Rémy Farge, formateur à la LDH

*L'été 2024 aura vu l'Europe sceller définitivement son avenir sur l'intelligence artificielle avec l'entrée en vigueur de l'AI Act. Une partie de ses dispositions seront applicables dès février 2025. Certains médias annonçaient, à tort, que l'usage de la reconnaissance faciale par la police serait alors autorisé. C'est en réalité le contraire : l'AI Act interdit l'identification biométrique à distance, en temps réel, par les forces de l'ordre. Plusieurs exceptions sont possibles, mais pour être appliquées, elles devront faire l'objet d'une loi nationale. La Belgique pourrait dès lors adopter un cadre plus protecteur des droits humains, en interdisant totalement ce dispositif. La Ligue des droits humains plaide en ce sens de même que pour une réflexion plus large sur la vidéosurveillance algorithmique.*

## La vidéosurveillance algorithmique bien implantée en Belgique

L'analyse vidéo basée sur l'IA suscite auprès de certains mandataires et administrations un engouement exceptionnel qui se traduit par de nombreux contrats entre institutions publiques et entreprises de la surveillance. La police judiciaire de la zone Bruxelles-Nord a fait le choix de l'entreprise Kinesense. Outre la reconnaissance faciale que le chef de corps disait ne pas utiliser lors d'un conseil de police en 2019, son logiciel permet de filtrer les personnes en fonction notamment du genre et de l'âge prédits. Les « personnes d'intérêt » peuvent aussi être marquées d'un tag, un marqueur, et tracées à travers les différentes vidéos.

Un des logiciels les plus connus est celui de l'entreprise israélienne Briefcam utilisé sur toute la planète. Des garde-frontières l'utilisaient déjà en Israël en 2015 et le ministère du Logement le déploie dans les quartiers palestiniens occupés de Jérusalem-Est selon l'ONG Who Profits. En Belgique, les polices d'Uccle et de Bruxelles-Ouest l'ont installé depuis 2019, et le CIRB (devenu Paradigm) en charge

de la transition numérique à Bruxelles vante le gain de temps qu'il offre aux policier·ères. Mais que promet-il concrètement ? Couplé à des vidéos, cet « outil » permettrait de « détecter, de suivre, d'extraire et de classer » un objet ou une personne, notamment en fonction des vêtements, de la morphologie et des visages. Il détecte aussi des comportements définis comme suspects. L'exemple type : le maraudage qui peut être détecté dès lors qu'une personne reste relativement immobile pendant une durée prédéfinie. Le problème pour beaucoup d'expert·es : ce type de système est un moyen inespéré d'identifier automatiquement et de sanctionner des personnes ou des comportements « indésirables » pour les autorités, même s'ils ne représentent aucun danger. À l'heure où la criminalisation des mouvements sociaux, mais aussi de la mendicité et de la circulation des personnes migrantes ne cesse de croître, les craintes d'un renforcement des inégalités dans l'espace public grandissent tout autant. Un nouvel exemple depuis avril 2024 et l'adoption du pacte migratoire : l'élargissement du fichier Eurodac permettra à l'avenir de conserver les images faciales en plus des empreintes digitales des personnes en exil (à partir de 6 ans) ayant réussi à atteindre les frontières de l'UE.

En France, le média Disclose a révélé que la police utilisait illégalement la reconnaissance faciale avec BriefCam. La fonction était activée par défaut depuis 2018. Côté belge, la société qui détient une licence d'importateur de ce logiciel et qui l'a installé à Courtrai a dû elle-même désactiver les droits pour cette fonctionnalité. Le magazine *Médor* nous apprenait qu'elle était aussi disponible par défaut.

## Ce que l'organe de contrôle ne contrôle pas

Au niveau fédéral, l'organe de contrôle de l'information policière (COC) est l'autorité de protection des données pour la police belge. Le 10 septembre 2024, son directeur F. Schuermans déclarait à Sudinfo qu'il acceptait que la police utilise la reconnaissance faciale, « mais dans un cadre strict ». À savoir, « dans le cadre d'une enquête précise où il s'agit de reconnaître le visage d'un suspect, en le comparant aux photos qui sont déjà dans les bases de données de la police ». Il justifiait cette acceptation limitée en se basant sur un article de la loi sur la fonction de police inséré en 2018 sur l'utilisation des données biométriques pour assurer l'identification certaine d'un·e suspect·e. Cette position surprend tant elle est en contradiction avec une analyse que le COC lui-même publiait en janvier 2022, bien après

l'introduction de cet article. Dans cet avis relatif à la proposition d'un moratoire sur la reconnaissance faciale, le COC considérait que « le cadre légal actuel n'offre de toute manière aucun fondement juridique (suffisant) permettant à la police [...] – et donc également au parquet et au juge d'instruction – de recourir à une telle technologie [...]. De fait, ni la loi sur la fonction de police, ni le Code d'instruction criminelle ni une quelconque autre loi (pénale) spéciale n'offre de lege lata un fondement juridique (suffisant) ». La LDH a interrogé le COC au début du mois d'octobre quant à cette contradiction. Plus d'un mois après, le message est resté lettre morte.

La criminologue Rosamunde Van Brakel soutient que les organes de contrôle de la police belge n'accordent pas suffisamment d'importance aux « préjudices socio-techniques de la surveillance algorithmique de la police »[1]. Selon elle, « le contrôle de la surveillance policière algorithmique devrait prêter attention aux choix politiques, éthiques et sociaux qui ont été faits », et ce au-delà d'un examen purement légal. Les affaires relatives à la reconnaissance faciale illustrent bien cette nécessité. D'un côté, c'est le COC qui a permis de mettre un terme au projet de la police fédérale à l'aéroport de Zaventem ou aux tests du logiciel Clearview AI, du fait de leur illégalité manifeste. Dans le même temps, dans son rapport sur le projet à l'aéroport, il tempère : « Si la police souhaite recourir aux nouvelles technologies – une idée à laquelle l'Organe de contrôle n'est évidemment pas opposé –, il relève de sa responsabilité de désigner le fondement juridique applicable et de soumettre à l'Organe de contrôle l'analyse de risques et d'impacts ». En évitant l'évaluation approfondie des risques de discriminations, d'inégalités sociales et des enjeux éthiques qui entourent cette technologie, le COC donne implicitement raison à la critique adressée par la chercheuse. Exit l'analyse des conséquences possibles, par exemple, sur les personnes en exil exposées au traçage et aux violences, sur les journalistes d'investigation souhaitant rencontrer leurs sources en sécurité, ou des groupes sociaux confrontés historiquement au racisme à toutes les étapes de la chaîne pénale.

## Des pratiques sauvages aux deux pieds dans la porte ?

Sous couvert d'encadrement juridique, l'AI Act donne une opportunité aux États membres de légaliser la reconnaissance faciale, non seulement a posteriori dans le cadre d'enquêtes mais aussi en temps réel.

1. Van Brakel, Rosamunde (2021). How to Watch the Watchers ? Democratic Oversight of Algorithmic Police Surveillance in Belgium. Surveillance & Society. 19.

La formation du futur gouvernement fédéral est une occasion que semble vouloir saisir la N-VA. En octobre 2024, *Le Soir* publiait les grandes lignes de la note « sécurité » rédigée par Bart De Wever et visiblement endossée par ses futurs partenaires gouvernementaux. Les mesures sécuritaires, voire autoritaires, foisonnent : interdictions judiciaires de manifester, déchéance de nationalité, tolérance zéro contre la drogue, mais aussi usage de la reconnaissance faciale. D'une part, les négociateurs fédéraux souhaitent la « facilitation » des « champs d'expérimentation » pour détecter des suspect·es ou des condamné·es. Impossible de ne pas penser aux pratiques « sauvages » observées sans cadre légal lors des deux projets tests précités. D'autre part, la note mentionne la création d'une nouvelle base de données afin d'identifier les « interdits de stade ». Cette dernière mesure avait opportunément été proposée en avril dernier par Lorin Parys, le CEO de la Pro League et… l'ancien vice-président de la N-VA.


**CAMÉRA DE SURVEILLANCE, BRUXELLES**
décembre 2021 © Aline Wavreille

Alors que l'on tournait presque la page de 2024, le ministre libéral Paul Van Tigchelt déposa le 17 décembre une 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 sur l'intelligence artificielle. La mise en œuvre pour laquelle il plaide ne vise pas à nous prémunir des dangers de la surveillance biométrique en l'interdisant, mais plutôt à « autoriser l'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives ».

La Belgique s'en tiendra-t-elle à l'interdiction de cette technologie, ou adoptera-t-elle une législation admettant cette nouvelle forme de surveillance biométrique ? Pour se préserver de tout fatalisme et éviter les informations erronées, rappelons que rien n'oblige les autorités à accepter le recours à la reconnaissance faciale. Poussée dans le dos par une mobilisation à laquelle tente de participer la campagne *Protect my face*, la Belgique pourrait faire le choix d'adopter une loi plus restrictive en faveur d'une protection renforcée des droits et libertés.