Aline Wavreille, chargée de communication à la Ligue des droits humains

Reconnaissance faciale : fuyez, vous êtes filmé·es… et identifié·es

La Ligue des droits humains, avec sept autres associations (la Liga voor mensenrechten, le MRAX, le Collectif Mémoire coloniale et lutte contre les discriminations, Genres pluriels, le CIRé, Tactic et Technopolice) a lancé, au printemps dernier, la campagne #Protectmyface visant à interdire l'usage de la reconnaissance faciale dans l'espace public bruxellois. Cette technologie biométrique n'est pas autorisée en Belgique mais les autorités ont pour projet de s'en équiper, les freins techniques sont contournés, plusieurs tests ont déjà été réalisés. Or, l'usage de la reconnaissance faciale dans l'espace public entravera durablement nos droits fondamentaux.

Caméras, logiciels et base de données

La reconnaissance faciale est une technologie que l'on associe encore parfois à de la science-fiction ou à des outils au service de dictatures lointaines. Pourtant, elle est aujourd'hui à portée de main des autorités belges, qu'elles soient fédérales, régionales ou locales. Toutes les caméras de surveillance peuvent potentiellement être dotées d'un logiciel de reconnaissance faciale. Cette technique d'analyse biométrique utilise les caractéristiques du visage (la longueur du front, l'écartement des yeux, les arêtes du nez, la distance entre la bouche et le nez, etc.) pour identifier une personne. Le système transforme les traits des visages en données biométriques et les compare avec celles qui composent la base de données. Pour utiliser la reconnaissance faciale, il faut donc trois éléments : des caméras, un logiciel de reconnaissance faciale et une ou plusieurs bases de données.

Autorisée ou pas ?

En Belgique, aucune loi n'encadre l'usage de la technologie de la reconnaissance faciale. Étant donné qu'elle est une technologie hautement attentatoire à la vie privée – puisqu'elle consiste à récolter et traiter des données à caractère personnel – elle n'est pas autorisée et doit être donc considérée comme illégale et interdite. Le COC, l'Organe de Contrôle de l'Information policière, épinglait dans son avis[1] concernant une proposition de moratoire de trois ans sur l'utilisation de logiciels et d'algorithmes de reconnaissance faciale sur les caméras de sécurité que : «*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) pour l'utilisation de la FRT dans le cadre de missions de police administrative ou judiciaire*».

Des tests… menés en toute illégalité

Cette technologie n'est pas autorisée mais il existe une volonté politique de lui fournir un cadre légal. La reconnaissance faciale suscite un grand intérêt du côté de la police. Quant à la ministre de l'Intérieur Annelies Verlinden, elle a déjà exprimé à plusieurs reprises sa volonté de permettre aux forces de police d'y avoir recours « pour faciliter, par exemple, la recherche de personnes disparues dont la vie est supposée en danger ». Et la ministre de se référer au cadre européen en cours d'élaboration : l'IA-Act. À la mi-juin, le Parlement européen a voté un texte qui encadrait les technologies de surveillance biométrique et a décidé d'interdire la reconnaissance faciale en temps réel, mais la décision se jouera ensuite dans les trilogues entre Parlement européen, Commission européenne et Conseil européen.

En attendant, la police fédérale a déjà mené plusieurs tests en Belgique qui ont été pour la plupart interrompus par le COC, l'Organe de Contrôle de l'Information Policière, parce que jugés illégaux. (Des tests souvent lancés sans en avoir sollicité l'avis du COC, alors que la loi l'y oblige).

1 https://www.organedecontrole.be/files/DA210029_Avis_F.pdf

Rétroactes. En 2017, puis en 2019, la police fédérale a réalisé des tests à l'aéroport de Zaventem. Ils visaient à repérer des suspects en matière de terrorisme et de criminalité organisée : « Nous allons comparer des photos d'auteurs (de crimes) connus, en des endroits spécifiques, sur place et en temps réel », expliquait à la RTBF la porte-parole de la Police fédérale Sarah Frederickx. En 2020, la police fédérale a également réalisé une septantaine de recherches avec le logiciel Clearview IA, très controversé, dans le cadre de réunions Europol. Une enquête du COC a également été ouverte[2].
Par ailleurs, selon une recherche menée par la KULeuven[3] en Flandre et en région bruxelloise, au moins 5 zones de police locale sur 86 répondantes, disposaient de la reconnaissance faciale en 2021, l'une d'elle affirmant même l'utiliser "souvent à très souvent".
En région bruxelloise, des zones de police utilisent notamment le logiciel "BriefCam", de la société israélienne du même nom, pour analyser, au moyen d'algorithmes, les images des caméras qui filment l'espace public bruxellois. La société BriefCam propose aussi un système de reconnaissance faciale, compatible avec une partie du réseau de caméras à Bruxelles. Il n'y a donc plus de frein "technique" au déploiement de la reconnaissance faciale et une volonté politique forte d'en faire usage dans un futur proche.

Libertés et droits fondamentaux menacés

D'importantes sommes d'argent sont donc investies dans du matériel de vidéosurveillance, l'infrastructure est déployée, puis testée. Quant à la question de l'impact sur la population et les droits des personnes : « Ces questions de droits arrivent toujours dans un second temps », observe Chloé Berthélémy, conseillère politique chez EDRI, European Digital Rights. « Il faut toujours un sursaut soit des organes de contrôle, soit du grand public pour que ces questions de cadre légal et de choix de société soient débattues dans l'arène politique, publique et médiatique. (...) Ces préoccupations cruciales arrivent beaucoup trop tard ».

Or, l'usage de la reconnaissance faciale dans l'espace public comporte des risques importants d'atteinte à la vie privée et à la liberté individuelle. « La technologie de reconnaissance faciale à des fins d'identifications, accoudée à une base de données massives qui répertorierait toute la population, c'est la fin de l'anonymat dans l'espace public », tranche Chloé Berthélémy. « Nous serions constamment identifié·es. Ce dispositif aurait des effets dissuasifs sur les personnes, dans l'exercice de leurs droits fondamentaux : avoir peur d'être fiché·e, simplement en circulant, s'auto-censurer dans ses comportements, comme celui d'aller à une manifestation, fréquenter des lieux de divertissement, etc. ».

« Chilling effect »

En Allemagne, selon EDRI, les autorités de la ville de Cologne ont déployé un système de reconnaissance faciale à proximité de bars LGBTQIA+, de lieux de culte (mosquées, synagogues, etc.) et de cabinets médicaux et d'avocat·es sans aucune justification légitime. « Est-ce que l'État a vraiment besoin de savoir tout cela à propos de nous ? », s'interroge Chloé Berthélémy. « La réponse est non. Le problème, c'est que ce genre de systèmes nous conduit vers ces usages ». Et ces usages produisent ce que l'on appelle un chilling effect que l'on peut traduire par effet dissuasif, paralysant ou « d'auto-censure ». Il a par exemple été observé lors d'une évaluation menée en Grande Bretagne sur l'utilisation de la reconnaissance faciale par la Police métropolitaine de Londres. « L'une des conclusions était l'impact sur la liberté de penser et la liberté de réunion », se souvient Rosamunde Van Brakel, criminologue et professeure à la VUB. « Ces technologies peuvent créer des « chilling effects » que l'on a déjà observés pendant les Jeux Olympiques de Vancouver au Canada en 2010. Des activistes figuraient sur une liste de surveillance et alors qu'ils n'avaient commis aucune infraction, ils étaient repérés dans la foule et étiquetés comme danger potentiel.

Par ailleurs, tou·tes les citoyen·nes ne sont pas égaux·ales face au contrôle social

2 https://www.organedecontrole.be/files/DIO21006_Rapport_Contr%C3%B4le_Clearview_F_00050441.pdf
3 https://www.researchgate.net/publication/355585410_Digitalisering_in_de_lokale_politie_in_Vlaanderen_en_Brussel_Waar_staan_we

et à la criminalisation des comportements. L'usage de cette technologie risque d'impacter surtout les groupes sociaux particulièrement affectés par la précarité et plus marginalisés : personnes migrantes, communauté LGBTQI+, minorités raciales, personnes sans-abri et de toutes personnes qui pourraient avoir une opinion, une identité, un statut administratif ou tout comportement dans l'espace public déterminé comme « non-conforme » à la norme dominante ou établie. L'expérience menée à Côme en Italie parle d'elle-même, le système de surveillance mis en place par la ville est entraîné pour repérer les comportements d'errance sur la voie publique.

Risques de glissement

Enfin, cette technologie implique d'importants risques : piratages de ces données à caractère personnel très sensibles, erreurs et reproduction des discriminations sexistes ou racistes induites par les conceptions sociales dominantes et les institutions qui les vendent et les utilisent, menace d'un glissement vers une surveillance de masse. Chloé Berthélémy, conseillère politique chez EDRI recadre : « On nous dit que les finalités premières de ce genre de surveillance visent la lutte contre le terrorisme ou la recherche d'enfants disparus. Ce sont tous deux des objectifs légitimes, qui devraient être des priorités. Mais la réalité, c'est qu'une fois les infrastructures mises en place, la pratique nous démontre qu'il y a systématiquement un glissement qui s'opère vers d'autres finalités. Si on vise les terroristes, pourquoi ne pas viser la criminalité grave ? Pourquoi ne pas installer des caméras dans le port d'Anvers pour lutter contre le narcotrafic ? Et puis dans tout le quartier autour ? Cette tentation de rentabiliser l'infrastructure est très présente, c'est très simple d'élargir les objectifs une fois l'exception acceptée : one size fits all ».

Chine, Iran, Russie, frontières européennes

De plus, l'efficacité de la reconnaissance faciale reste encore très relative en raison des dérives et des erreurs qu'elle engendre encore. En Grande-Bretagne, la reconnaissance faciale est utilisée depuis 2016. Trois ans plus tard, une première étude indépendante[4], réalisée par deux chercheurs de l'Université d'Essex sur l'usage de la reconnaissance faciale par la police de Londres a montré que 80 % des suspect·es signalé·es par le logiciel de reconnaissance faciale étaient en fait innocent·es. Le système identifiait régulièrement des personnes à tort, avec toutes les conséquences sociales et légales que cela peut induire. Les dérives de cette surveillance biométrique sont, par contre, bien documentées. En Chine, la reconnaissance faciale est un outil du contrôle social mis en place par les autorités. Le journal américain Wired révélait il y a quelques mois que l'Iran utilisait la reconnaissance faciale pour identifier les femmes qui refusent de porter le voile. La Russie cible également les opposant·es à la guerre contre l'Ukraine. N'allons pas si loin : l'Union européenne expérimente ces nouvelles technologies dans les hotspots en Grèce et en Italie, ces « camps de réception des migrant·es ». En plus des empreintes digitales des personnes migrant·es, il est prévu de récolter leurs images faciales à partir de 6 ans. Une technologie qui permet également de reconnaître les émotions des demandeur·es d'asile et de mesurer ainsi l'authenticité de leurs récits est testée aux frontières.

Quel modèle de société voulons-nous ?

Les entreprises qui développent ces technologies de surveillance biométrique ont le vent en poupe, elles poursuivent leurs démarches de séduction auprès des gouvernements, des autorités locales, etc. Et souvent, le manque d'expertise et la tentation de céder aux solutions-miracles guident les décisions politiques, qu'importent les risques et les dérives liés à l'usage de la reconnaissance faciale.
Pour la criminologue de la VUB Rosamunde Van Brakel, « *quand les forces de police se préparent à investir dans certaines de ces technologies, une évaluation non seulement légale mais aussi éthique doit avoir lieu. C'est le moment de se demander si l'on veut réellement cette technologie pour notre société. La police ne devrait pas être la seule à prendre cette position, il faudrait également mettre en place un comité éthique avec des représentant·es des communautés locales. J'ai l'impression que la façon dont les technologies sont en train d'être implantées en Belgique est pour l'instant anti-démocratique* ».

4 https://www.essex.ac.uk/research-projects/human-rights-big-data-and-technology/facial-recognition