Version (longue) de l'auteure de :

Myrtille Picaud, « La reconnaissance faciale : un marché en construction ? », Note de veille, *Futuribles*, 16.04.2020, https://www.futuribles.com/fr/article/reconnaissance-faciale-un-marche-en-construction/

La reconnaissance faciale : un marché en construction ?

L'utilisation de la reconnaissance faciale en Chine, notamment pour contrôler la minorité des Ouighours, ou dans le cadre du projet dit de « crédit social », a récemment attiré de fortes critiques de la communauté internationale, qui dénonçait la surveillance et le contrôle généralisés dans ce pays. Néanmoins, la reconnaissance faciale, dont le marché mondial est estimé à 7 milliards de dollars d'ici 2024[1], se développe dans de nombreux pays européens sans attirer de telles critiques. Quels enjeux pose l'utilisation de cette technologie ?

La reconnaissance faciale s'appuie sur une image (film ou photographie) pour modéliser des caractéristiques du visage sous forme numérique afin de définir un gabarit censément unique à chaque personne. Ce gabarit est comparé avec d'autres modèles de visages, afin de « reconnaître » un individu selon un modèle probabiliste. La reconnaissance faciale permet ainsi d'*authentifier* une personne, dans l'accès à un service ou à un espace : c'est le cas dans les aéroports, où la reconnaissance faciale permet d'attester si la personne passant le contrôle est bien la même que celle identifiée par son passeport. C'est aussi ce que prévoit ALICEM (Authentification en ligne certifiée sur mobile), « solution » d'identité certifiée en ligne que l'Etat souhaite mettre en œuvre afin d'accéder à différents services administratifs. Les dispositifs expérimentaux dans des lycées à Nice et Marseille reposaient sur le même principe pour contrôler l'entrée des élèves, mais ils n'ont pas été mis en œuvre suite à l'avis de la CNIL, qui les a considérés comme ni nécessaires, ni proportionnés. La reconnaissance faciale peut aussi permettre d'*identifier* des individus : par exemple pour connaître l'identité de personnes dans une foule, en comparant l'image de leur visage à des gabarits stockés dans un fichier. Cette technique est utilisée par la police londonienne pour repérer des personnes recherchées dans l'espace public (Fussey et Murray, 2019).

Alors que la CNIL appelle depuis 2018 à un débat sur les éléments techniques, juridiques et éthiques[2] de cette technologie, d'autres organisations, comme la Quadrature du Net ou la Ligue des Droits de l'Homme, demandent son interdiction. Elles soulignent en particulier la dimension invasive de cette technologie, qui transforme le visage en traqueur, ainsi que son invisibilité dans l'espace public, conférant à « l'Etat un pouvoir de contrôle total sur la population, dont il ne pourra qu'être tenté d'abuser contre ses opposant·es politiques et certaines populations »[3]. La reconnaisance faciale est une technologie basée sur le traitement de données biométriques – des données sensibles au sens du Règlement général sur la protection des données européen – et interdit sauf exception, par exemple avec le consentement des individus. Il est donc possible de mettre en œuvre, dans certaines conditions et quand cela est proportionné des solutions de reconnaissance faciale pour l'authentification, avec le consentement de la personne, et en lui offrant des solutions alternatives. L'utilisation dans l'espace public pour l'identification, et à des fins sécuritaire est soumise à la Directive Police-Justice est à ce jour interdite, car non encadrée par des textes. La CNIL appelait en novembre 2019 à « tracer des

[1] https://www.marketsandmarkets.com/Market-Reports/facial-recognition-market-995.html
[2] https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf
[3] https://www.laquadrature.net/2019/12/19/rf_securitaire/

lignes rouges au-delà desquelles aucun usage, même expérimental, ne peut être admis »[4]. La reconnaissance faciale avait par exemple été expérimentée auprès de volontaires lors du carnaval de Nice, afin de tester son efficacité.

La Commission Européenne souhaite encadrer (plutôt qu'interdire) ces systèmes d'identification biométrique à distance. En France, des représentants des pouvoirs publics et des membres de l'industrie de la sécurité appelle à légiférer pour l'autoriser, arguant du retard pris par rapport à ses concurrents dans des pays où le cadre légal est plus permissif. L'organisation des Jeux Olympiques et Paralympiques (JOP) par la France, en 2024, est présenté par les pouvoirs publics et les entreprises comme un événement « à risque » nécessitant une sécurité extraordinaire et donc la mise en œuvre de la reconnaissance faciale[5]. Les JOP font partie des « projets emblématiques et fédérateurs » autour desquels s'organise la politique industrielle de sécurité à horizon 2025 promue par le Comité de la filière industrielle de sécurité[6]. Ils pourraient justement leur fournir l'occasion de « lever les freins » juridiques empêchant la mise en œuvre de la reconnaissance faciale dans l'espace public.

Pourtant, l'usage de la reconnaissance faciale dans l'espace public, et à des fins sécuritaires, pose plusieurs questions : d'abord, par rapport aux inégalités que ces dispositifs sont susceptibles de créer. Pour ces raisons, leur usage soulève des enjeux éthiques et politiques, car ces technologies n'ont pas toujours prouvé leur efficacité mais sont mises en œuvre néanmoins. On peut ainsi interpréter leur développement à travers des enjeux économiques, en y voyant l'expansion d'un marché de la sécurité numérique.

La façon dont sont développés les algorithmes, selon les données de départ sur lesquelles ils s'appuient, contribue à la formation de « biais », qui reflètent en réalité des inégalités sociales : par exemple, les développeurs utilisent des visages pour entrainer les algorithmes qui surreprésentent les hommes ou les individus blancs. Pour cette raison, les algorithmes reconnaissent jusqu'à présent moins bien les femmes ou les personnes noires (Buolamwini, 2017). Ces biais, parfois difficiles à établir, peuvent poser de graves problèmes si la reconnaissance faciale est utilisée à des fins sécuritaires : l'algorithme peut détecter une correspondance alors qu'il ne s'agit pas de la bonne personne, ce qui conduit notamment au sur-contrôle des groupes les moins bien reconnus, comme les hommes noirs (Fussey et Murray, 2019), déjà sur-ciblés par les politique sécuritaires (Jobard et al., 2012). Pour cette raison, l'importance de créer des algorithmes « éthiques » a été soulignée, en recourant par exemple à des bases de données représentant les différents visages de la population, notamment en termes de genre et d'ethnicité[7], une solution technique envisageable à terme. Si l'analyse de ces biais est utile, elle présente néanmoins deux écueils.

Premièrement, en centrant la critique sur le fonctionnement des technologies, elle évacue toute discussion de leur nécessité réelle. A l'image de la vidéosurveillance, leur utilisation est justifiée par l'existence de risques, quoique leur efficacité ne soit pas prouvée (Castagnino, 2017 ; Gormand, 2017 ; Lemaire, 2019). Par exemple, le renseignement en amont serait plus efficace dans la prévention d'événements tels que des attentats. En outre, jusqu'à présent, les déploiements de reconnaissance faciale à des fins d'identification de personnes recherchées, au Royaume Uni notamment, témoignent d'une faible effectivité. Ainsi, la South Wales Police a déployé cette technologie lors des matches de football de la Ligue des Champions en 2017, à l'entrée des stades concernés. Le logiciel a généré 2632 alertes, signalant des personnes dans la

[4] https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf

[5] https://sd-magazine.com/grands-evenements/la-securite-des-jeux-olympiques-et-paralympiques-de-paris-2024

[6] https://www.cics-org.fr/wp-content/uploads/2018/01/3-CoFIS-politique-industrielle-nationale-Milipol-Paris-2017.pdf

[7] P. 19, https://ec.europa.eu/info/files/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

foule comme correspondant aux personnes recherchées. Or, 2554 de ces alertes, soit 97%, étaient erronnées et une seule arrestation a été effectuée, pour des milliers de personnes scannées[8]. Il est néanmoins envisageable qu'à terme, ces erreurs diminuent, à mesure que les algorithmes s'affinent et que ces technologies soient utilisées sur une période suffisante en conditions réelles.

Deuxièmement, l'analyse des « biais » techniques de ces technologies ne dit souvent rien des usages réels qui en sont faits et des différentes catégories de professionnels qui les utilisent, pour cibler quelles populations. Ainsi, le recours à cette technologie sera peut-être autorisé au départ dans des cas spécifiques. L'histoire des politiques sécuritaires témoigne toutefois de la circulation des dispositifs répressifs ou de surveillance, d'abord expérimentés sur des groupes sociaux ou dans des lieux qui éveillent peu de critiques, à l'instar des quartiers populaires ou des stades de football, avant d'être généralisés et utilisés aussi dans le cadre de manifestations politiques. Pour cela, le lien entre JOP et reconnaissance faciale doit nous interroger. Ces grands événements festifs sont souvent soutenus par le grand public, ce qui rend plus consensuel l'usage de dispositifs de surveillance et de répression destinés à les protéger et limite la possibilité de débattre de l'opprtunité du recours à ces technologies. Mises en œuvre pour l'événement, elles sont souvent ensuite pérennisées lorsqu'il se termine. Par ailleurs, les JOP sont depuis longtemps une vitrine pour le marché de la sécurité. Si les technologies ne sont pas toujours efficaces, comme cela fut le cas en Grèce en 2004 (Bennett et Haggerty, 2011), ces événements permettent de tester en taille réelle et contribuent à en banaliser l'usage. Ils sont souvent suivis par la signature de nombreux contrats de sécurité, qui sont déjà anticipés par les membres de l'industrie de la sécurité et les représentants des pouvoirs publics, qui souhaitent valoriser l'offre d'entreprises françaises[9].

On peut ainsi analyser la mise en avant croissante de la reconnaissance faciale à l'aune du juteux marché qu'elle recouvre. Or, dans le cas de la sécurité, ces marchés reposent en grande partie sur des clients publics, en particulier en France : forces de l'ordre, administrations nationales ou locales, etc. Alors que les dépenses publiques connaissent de fortes réductions, on peut se demander si ce marché de la sécurité numérique est bien une priorité, par rapport à d'autres secteurs qui influent également, mais plus indirectement, sur la sécurité des personnes (santé, éducation, etc.). Le recours à la reconnaissance faciale participe également de la recomposition des rapports entre public et privé dans la gestion de missions de sécurité régaliennes. Ainsi, dans les aéroports de Paris, 95 nouveaux sas de Passage automatisé rapide aux frontières extérieures, qui utilisent la reconnaissance faciale pour comparer un individu et la photo du passeport, auraient été installés en 2018, remplaçant 75 sas qui recourraient à la reconnaissance d'empreintes digitales. Cette technologie est développée par Gemalto, entreprise spécialisée dans la biométrie et rachetée par Thales (aérospatial, sécurité et défense) pour 4,8 milliards d'euros en 2019. Le coût de ces sas, estimé à environ 7,6 millions d'euros[10], est intégralement financé par les Aéroports de Paris, et non par l'Etat, évitant à ce dernier de rémunérer des fonctionnaires à la police aux frontières pour effectuer des contrôles similaires. Si l'exploitation privée de ces technologies se fait en lien avec la forces de l'ordre et l'Etat, elle témoigne

[8] Voir les données fournies par la South Wales Police, http://afr.south-wales.police.uk/cms-assets/deployments/uploads/All-Deployments.pdf.

[9]Ainsi, selon Coralie Héritier, Directrice Générale d'IDnomic, entreprise proposant des logiciels d'analyse de données biométriques, « La France dispose d'un savoir-faire éprouvé et de la technologie destinée et adaptée à la sécurisation des grands événements. Les JO de 2024 sont une excellente occasion pour la filière sécurité française de gagner des parts de marché à l'international », https://sd-magazine.com/grands-evenements/la-securite-des-jeux-olympiques-et-paralympiques-de-paris-2024.

[10] Pour 95 sas à eniron 80 000€, sans compter l'entretien, voir https://www.businessinsider.fr/vacances-controle-travaux-aeroport-paris/.

toutefois du poids croissant d'entreprises privées dans le développement et la gestion de missions de contrôle.

Finalement, la mise en œuvre de cette technologie questionne aussi les usages futurs des espaces publics, en particulier dans les villes. Le développement de la reconnaissance faciale dans la gestion d'espaces d'accès public, mais gérés par des entreprises privées, comme les gares, le métro, les centres commerciaux (Bonnet, 2012), incite aussi à penser les croisements entre enjeux économiques et sécuritaires dans le contrôle des espaces. Dans quelle mesure l'identification de personnes dans ces espaces peut-elle être soumise à des logiques économiques, qui excluent des individus vus comme indésirables à cause de leur pauvreté par exemple ? En outre, le développement de caméras de surveillance (ex. Ring d'Amazon) et de logiciels de reconnaissance faciale destinés aux particuliers, témoigne aussi des risques de l'extension et de l'éclatement de cette surveillance, bien au-delà des acteurs traditionnels de la sécurité, et de façon difficilement contrôlable.

Ainsi, les innovations technologiques doivent être analysées à l'aune des usages qui en sont faits, en examinant quelles populations et espaces sont ciblés, et par qui. Il s'agit d'aller plus loin que les discours, comme ceux de la Commission Européenne, sur l'éthique ou la transparence techniques des technologies, qui font fi de ces questions, afin d'initier un débat véritable sur les enjeux de la reconnaissance faciale et sur la croissance exponentielle de l'industrie de la sécurité numérique, sans se laisser aveugler par l'attrait de ce marché.

Bibliographie

BENNETT, C.J., HAGGERTY, K.D. (dirs.), 2011, *Security Games: Surveillance and Control at Mega-Events*, New York, Routledge.

BONNET F., 2012, « Contrôler des populations par l'espace ? Prévention situationnelle et vidéosurveillance dans les gares et les centres commerciaux », *Politix, 97*, 1, p. 25-46.

BUOLAMWINI J.A., 2017, « Gender Shades: Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers », Mémoire de master, Master of Science at the Massachusetts Institute of Technology, MIT.

CASTAGNINO F., 2017, *Les chemins de faire de la surveillance : une sociologie des dispositifs de sécurité et de sûreté ferroviaires en France*, Thèse de sociologie, Marne la Vallée, Université Paris-Est.

FUSSEY P., MURRAY D., 2019, « Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology », Essex, University of Essex.

GORMAND G., 2017, *L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier*, Thèse d'administration publique, Université Grenoble Alpes.

JOBARD F., LEVY R., LAMBERTH J., NEVANEN S., 2012, « Mesurer les discriminations selon l'apparence : une analyse des contrôles d'identité à Paris », *Population*, *67*, 3, p. 423–451.

LEMAIRE É., 2019, *L'œil sécuritaire. Mythes et réalités de la vidéosurveillance*, Paris, La Découverte.