CENTRE D'ÉTUDES
JACQUES GEORGIN

Le Centre d'Études Jacques Georgin est un centre d'éducation permanente reconnu par la Fédération Wallonie Bruxelles
ASBL Centre d'Etudes Jacques Georgin, 127, chaussée de Charleroi, 1060 Bruxelles
N° entreprise 0412.759.942. RPM: Tribunal de l'entreprise francophone de Bruxelles. BE30 7320 3232 6111

Note d'analyse 9 – 24 du Centre d'études Jacques Georgin

«Vers une légalisation de la reconnaissance faciale en Belgique ? Enjeux et stratégies»

Bruxelles, le 20 septembre 2024

Christophe Dubois, Directeur ff. du Centre d'Études Jacques Georgin

Avant-propos

Consécutivement aux rencontres qui ont été menées avec de nombreux acteurs de la société civile, parmi lesquels Rémy Farge, actif au sein de la Ligue des droits humains en qualité de formateur, ainsi qu'à un débat portant sur l'IA auquel il a participé en qualité d'intervenant, le CEG s'est attelé à étudier les enjeux liés à la légalisation de la reconnaissance faciale en Belgique. Il s'agit du sujet traité par la présente note d'analyse.

Outre l'apport d'une définition claire et une identification précise des fonctionnalités offertes par la reconnaissance faciale, cette note fait le point sur son cadre légal actuel, tant au niveau européen qu'au niveau de notre territoire. Ainsi, s'il existe – actuellement – une réglementation stricte interdisant l'utilisation de celle-ci sur le territoire de l'Union européenne, notre note d'analyse démontre que, bien plus qu'une volonté d'y recourir, certains pays ont procédé à des expériences pilote, voire continuent d'exploiter des fonctionnalités dérivées de cette dernière, en dépit des nombreuses questions éthiques soulevées par son utilisation.

Enfin, au-delà des atteintes portées à nos droits ainsi qu'à nos libertés fondamentales, la question de la légalisation de la reconnaissance faciale fait l'objet d'un enjeu économique majeur. En effet, en cas de feu vert à sa légalisation, les retombées économiques pourraient être très importantes pour les entreprises qui développent des logiciels d'analyse pour images de vidéosurveillance.

1. Contexte général

La reconnaissance faciale est aujourd'hui à notre portée car toutes les caméras de surveillance peuvent potentiellement être dotées d'un logiciel de reconnaissance faciale. Pour utiliser la reconnaissance faciale, il ne faut que trois éléments : des caméras, un logiciel de reconnaissance faciale et une ou plusieurs bases de données. En Belgique, aucune loi n'encadre l'usage de la technologie de la reconnaissance faciale. Et pourtant selon une recherche menée par la KULeuven 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'elles 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.

2. Qu'est-ce que la reconnaissance faciale ?

L'Autorité de protection des données définit la reconnaissance faciale comme *une technique permettant d'authentifier ou d'identifier une personne sur la base des traits de son visage : - Par "authentifier", on entend : vérifier qu'une personne est bien qui elle prétend être.* Utilisé aux contrôles d'accès, par exemple, un tel système détermine si l'identité obtenue au moyen de la reconnaissance faciale correspond à l'identité précédemment stockée dans la base de données. Identifier permet de retrouver une personne au sein d'un groupe, dans un lieu, une image ou une base de données. Ce système analyse si le visage présenté correspond aux modèles enregistrés dans la base de données sur la base de "critères de similarité". La reconnaissance faciale effectue des analyses à partir des caractéristiques du visage, telles que la longueur du visage, l'écartement des yeux, l'arête du nez, la distance entre la bouche et le nez, etc. Le système convertit ces caractéristiques faciales en données biométriques et les compare aux données collectées et stockées dans une base de données. En principe, toute caméra peut être équipée d'un logiciel de reconnaissance faciale. Les analyses peuvent être effectuées en temps réel ou a posteriori, sur la base d'images stockées. En principe, il faut donc trois éléments pour utiliser la reconnaissance faciale : une caméra, un logiciel de reconnaissance faciale et une ou plusieurs bases de données. Il est important de souligner qu'il s'agit clairement de données biométriques – des données uniques, propres à une personne. Ces données sont donc considérées comme des données personnelles très sensibles en vertu des lois européennes et nationales sur la protection de la vie privée.

3. Que dit la loi au niveau européen ?

Aujourd'hui, le cadre légal est fixé par le Règlement sur l'Intelligence artificielle, entré en vigueur le 1er août 2024, mais avec dispositions entrant en vigueur dans les 3 ans.

Ainsi, l'AI Act (ou RIA), qui établit des règles harmonisées en matière d'intelligence artificielle (IA), a été adopté le 21 mai 2024 et publié au journal officiel européen le 12 juillet 2024. Il entrera en application progressivement à partir du 2 août 2026 et jusqu'en 2027, bien que certaines dispositions seront applicables dès février 2025. Il apporte également des principes directifs (complémentaires au RGPD) visant à réguler l'usage des systèmes de reconnaissance faciale qui est un des domaines d'application de l'intelligence artificielle, et, notamment, une distinction entre les systèmes d'identification biométrique à distance « en temps réel » et « *a posteriori* », en son article 3 « Définitions ».

De façon générale, l'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives est interdite par principe. À la manière du RGPD, l'AI Act admet des exceptions à ce principe pour justifier le recours à de tels outils :

1. la recherche ciblée et spécifique de victimes d'enlèvement, de la traite ou de l'exploitation sexuelle d'êtres humains, ainsi que la recherche de personnes disparues ;
2. la prévention d'une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique d'individus, ou d'une menace réelle et actuelle ou réelle et prévisible d'attaque terroriste ;
3. la localisation ou l'identification d'une personne soupçonnée d'avoir commis une infraction pénale suffisamment grave (voir l'annexe II du texte, par exemple : terrorisme, trafic de stupéfiant, homicide volontaire).

L'instauration d'un cadre au niveau européen va de pair avec une indispensable complémentarité avec les lois nationales. En effet, si le règlement européen interdit déjà, en principe, l'usage de la reconnaissance faciale, il ouvre la porte à des dérogations ainsi qu'à des législations nationales. Ainsi, l'AI Act renvoie aux États membres la responsabilité de préciser les cas d'autorisation du recours à la reconnaissance faciale en temps réel dans le cadre de ces exceptions, qui seront subordonnés à une autorisation préalable octroyée par une autorité judiciaire ou administrative indépendante. Il reviendra donc à chaque Etat membre d'adopter des textes précisant la possibilité, par exception, de recourir à des systèmes d'identification biométrique à distance à des fins répressives.

Le texte européen classe également les systèmes d'identification biométrique à distance, les systèmes d'IA destinés à être utilisés à des fins de catégorisation biométrique et les systèmes d'IA destinés à être utilisés pour la reconnaissance des émotions comme des systèmes d'IA à haut risque ; mais également, plus largement, tous les systèmes d'IA destinés à être utilisés par les autorités répressives pour le profilage de personnes physiques, à des fins d'évaluation du risque qu'une personne commette une infraction, qu'une personne devienne une victime, etc. (voir annexe III).

La classification de 'systèmes d'IA à haut risque implique la mise en œuvre d'un système de gestion des risques nécessitant un examen et une mise à jour périodique.

Ces systèmes doivent viser à :

- identifier les risques connus et raisonnablement prévisibles ;
- estimer et évaluer les risques identifiés ; et
- adopter des mesures appropriées et ciblées de gestion des risques conçues pour répondre aux risques identifiés.

Cette classification implique également la réalisation d'essais en conditions réelles et impose des exigences en termes de qualité des jeux de données utilisés. Elle requiert également la rédaction d'une documentation technique et la mise en place d'une journalisation / traçabilité des opérations réalisées par le biais de ce système. Enfin, ces systèmes doivent permettre un contrôle *effectif* par des *personnes physiques* pendant leur période d'utilisation.

En France, il existe une proposition de loi relative à la reconnaissance biométrique dans l'espace public. Les textes en vigueur apportent bien des lignes directrices en matière d'usages interdits ou autorisés. Ils mériteraient toutefois d'être complétés, notamment en droit interne afin de clarifier les exceptions aux principes d'interdiction, offrant explicitement aux opérateurs des « lignes rouges »

ne devant être franchies. A cet effet, on relèvera que la CNIL appelle depuis 2018 à un débat démocratique sur les nouveaux usages des caméras vidéo et à un réexamen d'ensemble des dispositions applicables en droit français afin d'apporter une réponse appropriée à l'ensemble des techniques et usages nouveaux mentionnés ci-dessus.

Un rapport du Sénat publié le 10 mai 2022 préconise également un encadrement précis de l'utilisation de la reconnaissance biométrique visant à empêcher les dérives vers une société de surveillance. Les rapporteurs considèrent qu'il est indispensable de fixer dans la loi quatre interdictions indistinctement applicables aux acteurs publics et privés :

- Interdiction de la notation sociale ;
- Interdiction de la catégorisation d'individus en fonction de l'origine ethnique, du sexe ou de l'orientation sexuelle ;
- Interdiction de l'analyse d'émotions ;
- Interdiction de la surveillance biométrique à distance en temps réel dans l'espace public (sauf exceptions limitées au profit de forces de sécurité, en particulier lors de manifestations sur la voie publique ou aux abords des lieux de culte).

Dans ce rapport, le Sénat recommande, notamment, l'adoption d'une loi d'expérimentation (c'est-à-dire une loi soumise à un calendrier d'évaluation) pour déterminer les usages de la reconnaissance biométrique et fixer des « lignes rouges » à ne pas franchir. Une proposition de loi relative à la reconnaissance biométrique dans l'espace public a été adoptée en première lecture par le Sénat le 12 juin 2023 et est, donc, toujours en cours d'examen.

Cette proposition de loi envisage de limiter juridiquement l'utilisation des technologies de reconnaissance faciale selon les conclusions du rapport d'information adopté par la commission des lois en mai 2022. Elle s'inscrit dans un objectif général de régulation et de cadrage de l'utilisation de la reconnaissance biométrique par les pouvoirs publics.

Le RGPD et l'IA Act se révèlent une source précieuse d'identification de la règlementation applicable à ces nouveaux usages vidéo "algorithmiques". La proposition de loi pendante devant le Parlement français, si elle est adoptée, viendra utilement préciser le cadre applicable aux cas d'utilisation par les pouvoirs publics (notamment la vidéo protection d'évènements à grande échelle, dans les lieux publics, etc.), mais également par les opérateurs privés. Le rapport du Sénat visant en effet les opérateurs publics comme privés, les acteurs commerciaux bénéficieraient également d'un cadre clair relatif aux technologies et cas d'usages variés résultant de ces systèmes vidéo « intelligents », qu'ils impliquent ou non des traitements de données biométriques.

4. Que dit la loi à propos de la reconnaissance faciale en Belgique ?

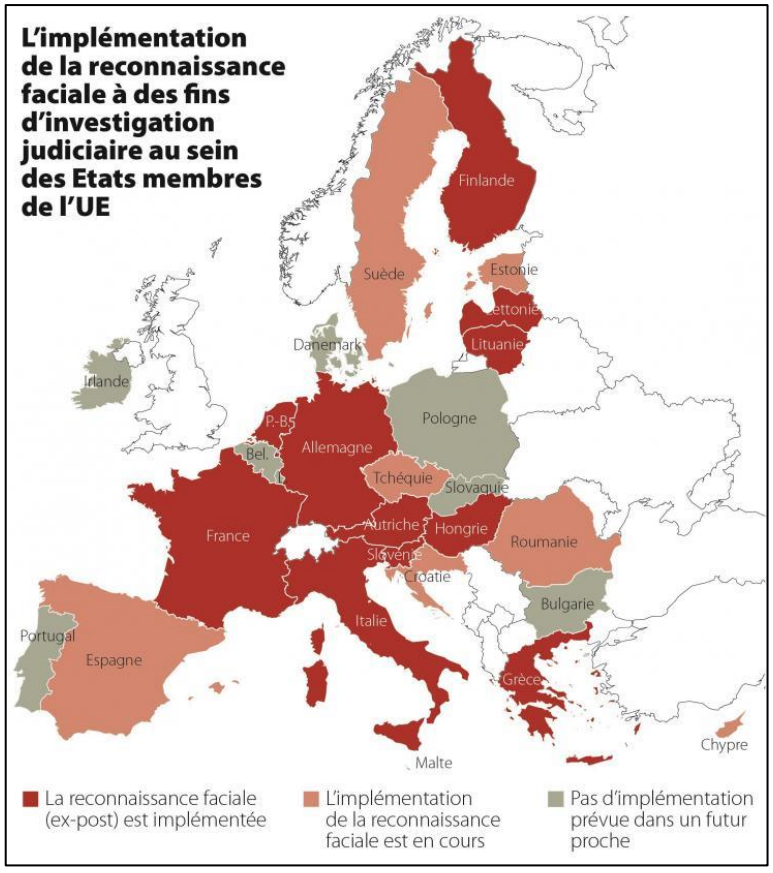
Actuellement, en Belgique, aucune loi n'encadre l'usage de la technologie de la reconnaissance faciale. Étant donné qu'elle est une technologie hautement attentatoire à la vie privée – puisqu'elle consiste à récolter et traiter des données à caractère personnel – elle n'est pas autorisée et doit être donc considérée comme illégale et interdite. Le COC – l'Organe de contrôle de l'information policière – l'a lui aussi encore souligné récemment. En mai 2020, un projet de résolution déposé au parlement fédéral demandait un moratoire de trois ans sur l'utilisation de logiciels et d'algorithmes de reconnaissance faciale dans les caméras de sécurité fixes ou mobiles installées dans l'espace public et les lieux privés. Dans son avis sur cette résolution, le COC souligne 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 technologie de reconnaissance faciale dans le cadre de missions de police administrative ou judiciaire. »

5. Qu'en est-il de l'utilisation de la reconnaissance faciale en Europe ?

Lors de cette dernière décennie, il semblerait que la mise en place de dispositifs sécuritaires reposant sur l'identification par reconnaissance faciale ou sur d'autres formes de technologies d'analyses biométriques (capteurs de mouvements, de sons, d'émotions, etc.) ait connu un véritable essor. Ainsi, dans son édition du 25 octobre 2021, le journal Le Soir nous apprenait que le groupe des Verts/ALE au Parlement européen avait commandé une enquête à cet effet. Cette dernière, dirigée par le chercheur Francesco Ragazzi, professeur associé en relations internationales à l'Université de Leiden (Pays-Bas), faisait état que *dans plusieurs pays d'Europe, 11 sur 27 pour être précis, la reconnaissance faciale à des fins d'identification de suspects dans le cadre d'investigations judiciaires est effectivement déjà une réalité – et elle le sera bientôt au sein de 7 autres. Ainsi, les polices d'Autriche, de Finlande, de France, d'Allemagne, de Grèce, de Hongrie, d'Italie, de Lettonie, de Lituanie, de Slovénie et des Pays-Bas utilisent des technologies de reconnaissance faciale pour l'identification a posteriori dans leurs enquêtes criminelles. La Croatie, Chypre, la République tchèque, l'Estonie, le Portugal, la Roumanie, l'Espagne et la Suède devraient suivre dans un futur proche. Sur ce plan, la Belgique (qui ne l'autorise pas) fait ainsi office d'exception au sein de l'UE. À contrario, en Allemagne, cela fait déjà plus de dix ans que des croisements entre la base de données policière nationale et des images de caméras peuvent être effectués via analyse biométrique, dans un cadre défini d'enquête. Attention, on ne parle a priori pas ici de tentatives d'identification « en temps réel » sur base d'images filmées en direct, mais d'analyses « ex-post », c'est-à-dire sur base d'images enregistrées qui sont consultées dans le cadre d'une enquête*.

Selon Le Soir, *ce type d'usage ne permet pas de parler de « surveillance de masse » à proprement parler, ce n'est pas le cas selon eux du recours à la reconnaissance faciale « en live », qui induit un flicage beaucoup plus généralisé. Or, cette forme de surveillance gagne aussi du terrain. L'épisode belge de l'installation de caméras « intelligentes » dans l'aéroport de Zaventem l'illustre bien. Ainsi, un dispositif « expérimental » de la police fédérale fut mis en place en 2017 mais ne fut amené qu'en 2019 à la connaissance du COC, l'Organe de contrôle de l'information policière belge. Un logiciel analysait en direct les images dans le but de repérer la présence d'éventuels individus « blacklistés ». Le COC a fini par déclarer l'usage illégal et le dispositif fut désactivé, mais restera en place. La mésaventure belge n'a pour autant pas refroidi tout le monde. Après une modification de sa législation en 2019,*



https://www.lesoir.be/402394/article/2021-10-25/la-reconnaissance-faciale-setend-de-plus-en-plus-en-europe

la Hongrie a notamment ouvert la voie à la reconnaissance faciale « en live » avec son projet « Dragonfly » qui repose sur une centralisation massive de bases de données civiles et policières, couplée à des recherches « en live » à partir d'un réseau de 35.000 caméras disposées à Budapest.

Cette enquête, menée par le Professeur Ragazzi, a permis également la réalisation d'une cartographie qui recense les projets s'appuyant sur les technologies biométriques. (Voir carte ci-contre)

Enfin, à l'occasion des Jeux Olympiques et Paralympiques de Paris, la France a franchi une nouvelle étape en légalisant la vidéosurveillance algorithmique. Concrètement, des caméras alimentées par l'intelligence artificielle ont analysé en temps réel les mouvements afin de détecter des situations "anormales". Cette loi, adoptée en procédure accélérée sans véritable débat public, positionne la France comme le premier État membre de l'Union européenne à légaliser ce type de surveillance à titre expérimental. Cela représente un tournant majeur qui ouvre la voie à l'utilisation de technologies encore plus intrusives telles que la reconnaissance faciale.

6. La reconnaissance faciale n'est pas réglementée en Belgique. Et pourtant…

En Belgique, aucune loi n'encadre l'usage des technologies de reconnaissance faciale par les autorités publiques. Pourtant, la reconnaissance faciale a déjà été utilisée par la police belge à plusieurs reprises. En 2017 et en 2019, la reconnaissance faciale a été testée par la police fédérale à l'aéroport de Zaventem. En 2019 et 2020, la police fédérale a réalisé une septantaine de recherches avec le logiciel controversé Clearview AI[1]. L'Organe de contrôle de l'information policière exigera la fin de ces expérimentations, aucun fondement juridique ne les autorisant.

Selon une recherche réalisée en 2021 par la KULeuven auprès des zones de police des régions flamande et bruxelloise, au moins 5 zones sur les 86 qui ont répondu disposaient de la reconnaissance faciale, l'une d'elle affirmant même l'utiliser souvent à très souvent.

La Région bruxelloise utilise le logiciel d'analyse de contenu vidéo BriefCam[2] qui permet de détecter, suivre et extraire tout objet en mouvement. L'entreprise israélienne qui le vend propose aussi des technologies de reconnaissance faciale. Par ailleurs, la ministre fédérale de l'Intérieur a déjà exprimé sa volonté d'y avoir recours « à condition que des garanties soient suffisantes en termes de respect des droits de l'homme ».

7. La reconnaissance faciale menace nos libertés

L'usage de cette technologie dans nos rues nous rendrait identifiables et surveillés en permanence. Cela revient à donner aux autorités le pouvoir d'identifier l'intégralité de sa population dans l'espace public, ce qui constitue une atteinte à la vie privée et au droit à l'anonymat des citoyennes et citoyens. La surveillance musèle la liberté d'expression et limite les possibilités de se rassembler, par exemple lors de manifestations. La reconnaissance faciale impactera surtout les groupes sociaux particulièrement affectés et marginalisés : personnes migrantes, communauté LGBTQI+, minorités raciales, personnes sans-abri, etc.

---

[1] Clearview AI est une entreprise américaine spécialisée dans la reconnaissance faciale. Elle fournit un logiciel basé sur une technologie qu'elle développe permettant de rechercher un visage parmi une base de données de plus de vingt milliards d'images, obtenues via *web scraping* sur Internet et notamment sur les réseaux sociaux.

[2] Briefcam est une entreprise israélienne détenue par Canon qui développe un logiciel d'analyse pour images de vidéosurveillance.

D'autres risques inhérents à cette technologie :

- risques quant au stockage des données : les risques de piratages informatiques visant ces données biométriques très sensibles sont importants et l'actualité belge a, de nombreuses fois, montré que les données récoltées par les autorités publiques n'étaient pas à l'abri de ces piratages ;

- risques d'erreurs et de discriminations accrues : les études montrent que cette technologie reproduit les discriminations sexistes ou racistes induites par les conceptions sociales dominantes et des institutions qui les vendent et qui les utilisent. En effet, la reconnaissance faciale est réputée pour fonctionner relativement bien sur les visages des hommes et femmes blancs, mais révèle des taux d'imprécisions élevés pour les personnes non blanches, surtout chez les femmes. ;

- risques de normalisation et de glissement vers la surveillance de masse : le déploiement des technologies de surveillance avance à coups de projets pilotes qui précèdent les cadres légaux, puis sont ensuite régularisés, souvent sans débat démocratique.

8. En Belgique, une résistance face à la légalisation de la reconnaissance faciale qui s'organise

La Ligue des droits humains et sept autres associations ont lancé la campagne #Protectmyface pour interdire l'utilisation de la reconnaissance faciale dans l'espace public à Bruxelles. Bien que cette technologie ne soit pas autorisée en Belgique, les autorités envisagent de l'adopter, ayant déjà réalisé plusieurs tests malgré les obstacles techniques. L'utilisation de la reconnaissance faciale dans l'espace public pose une menace sérieuse pour nos droits fondamentaux.

Ces associations ont soumis une pétition au Parlement bruxellois.

Elles commencent par définir la reconnaissance faciale. Selon elles, cette dernière est *une technologie qui permet l'identification des personnes sur la base de l'analyse de caractéristiques de leurs visages. Les algorithmes de ces systèmes identifient ou confirment l'identité de personnes présentes via la consultation d'une base de données.*

Pourquoi la Ligue des droits humains a-t-elle adressé sa pétition au Parlement bruxellois?

Si une modification de cadre légal permettant l'utilisation de la reconnaissance faciale doit nécessairement être votée au niveau fédéral, la région bruxelloise s'est, quant à elle, vue confier d'importantes responsabilités en matière de prévention et de sécurité. Selon la Ligue des droits humains, la Région adopte de plus en plus une politique sécuritaire, notamment avec la centralisation de la vidéosurveillance régionale.

Cette pétition* demande au Parlement bruxellois :

- d'interdire la reconnaissance faciale dans les lieux publics et son utilisation par les autorités à des fins d'identification, quelles que soient les réformes à venir ;

- qu'une audition devant le Parlement de la Région de Bruxelles-Capitale soit accordée à la LDH.

*(Pétition déposée avec les associations suivantes : Ciré, Genres Pluriels, Liga voor Mensenrechten, Ligue des droits humains, Mémoire coloniale et lutte contre les discriminations, MRAX, Tactic, Technopolice.be.)

9. Quelles suites pour cette pétition ?

Cette pétition a été déclarée recevable le 6 mars 2023 et publiée le même jour sur la plateforme democratie.brussels.

En date du 23 mai 2023, elle a recueilli le soutien de plus de 1.000 personnes résidant en Région de Bruxelles-Capitale et âgées d'au moins 16 ans.

En conséquence, les pétitionnaires ont été auditionnés le 13 juin 2023 par la commission des Affaires intérieures, chargée des Pouvoirs locaux, de la Sécurité et de la Prévention, des Cultes, de la Simplification administrative, du Transport rémunéré de personnes et de la Lutte contre l'incendie et l'Aide médicale urgente.

10. Une technologie qui comporte, pourtant, de nombreux avantages

En dépit des craintes et questionnements légitimes qu'elle soulève, la reconnaissance faciale peut offrir la possibilité de rendre nos vies plus pratiques et confortables. Ainsi, au lieu d'avoir à entrer un mot de passe sur nos téléphones ou d'avoir à montrer une pièce d'identité à l'aéroport, nos visages permettent de vérifier qui nous sommes.

À titre d'exemple, au Japon, quatre gares de la ville d'Osaka ont mis en place des systèmes de reconnaissance faciale afin de gérer l'entrée des voyageurs, en scannant leur visages sans que ces derniers n'aient à utiliser leur cartes d'identité. Les membres du personnel interrogés arguaient que « le fait que les passagers voyageant avec de grands bagages puissent simplement montrer leur visage sans avoir à chercher leurs billets constitue un avantage ».

Un autre argument en faveur de la reconnaissance faciale porte le caractère simple et facile des processus internes d'authentification biométrique à destination des usagers. Ainsi, placer un doigt sur un scanner et déverrouiller son compte en quelques secondes prends beaucoup moins de temps que de taper un long mot de passe que de nombreux utilisateurs oublient fréquemment. Le risque d'oublier ses propres données biométriques étant nul.

En matière de sécurité, les données biométriques permettent de savoir précisément si une personne est en train d'accéder à un service ou de payer une transaction. À cet égard, ceux qui défendent l'utilisation des données biométriques estiment que les mots de passe, PIN et autres informations d'identification peuvent être violées et piratées, ce qui permet aux fraudeurs d'accéder aux comptes reposant sur ces méthodes d'authentification.

11. Quel est l'enjeu économique qui se cache derrière la reconnaissance faciale ?

Les progrès technologiques croissants et la demande croissante de surveillance des systèmes pour améliorer sécurité et sécurité sont les principaux facteurs attribuables à la croissance du marché de la reconnaissance faciale. Data Bridge Market Research[3] analyse que le marché de la reconnaissance faciale affichera un taux de croissance annuel composé (TCAC)[4] de 16,10 % pour la période de prévision 2021-2028. Cela signifie que la valeur du marché de la reconnaissance faciale atteindra 15 milliards de dollars d'ici 2028.

[3] Data Bridge Market Research est une société d'études de marché et de conseil. Sa base de données contient des milliers de statistiques et d'analyses approfondies sur plus de 200 secteurs et plus de 5 000 marchés dans 75 grands pays du monde.

[4] Le TCAC (taux de croissance annuel composé) est le taux moyen de croissance des revenus, des ventes ou des investissements au fil du temps. Le TCAC prend en compte les effets des intérêts composés et des taux de croissance exponentiels.

Selon DBMR, la reconnaissance faciale est *une technologie utilisée pour l'authentification et l'identification des individus. La reconnaissance faciale est une technologie biométrique utilisée pour comparer les caractéristiques du visage d'une image avec la base de données faciale stockée. Généralement utilisée à des fins de sûreté et de sécurité, l'avènement de la technologie de reconnaissance faciale a amélioré l'efficacité et l'efficience des systèmes de sécurité. La popularité croissante de cette technologie a conduit à son intégration dans les smartphones.*

A. Tendances du marché de la reconnaissance faciale

La vente au détail et le commerce électronique devraient détenir une part importante

Ainsi, même si la technologie de reconnaissance faciale na pas initialement absorbé une demande massive du secteur de la vente au détail, elle a offert un potentiel suffisant à cette technologie au cours des dernières années. Les progrès dans trois domaines techniques, les réseaux de neurones, le big data et les unités de traitement graphique, ont joué un rôle important dans l'utilisation généralisée de la technologie de reconnaissance faciale dans le secteur. Par exemple, les détaillants de vêtements exploitent la technologie pour proposer des produits personnalisés aux clients visitant leurs magasins.

La technologie de reconnaissance faciale devrait aider les détaillants à analyser l'humeur et les expressions faciales de différents SKU (Stock Keeping Unit), c'est-à-dire l' identifiant unique pour un élément détenu par une entreprise, et à améliorer davantage leur expérience d'achat, en empêchant le vol et le vol à l'étalage, car la technologie contribue à accroître la sécurité au niveau du magasin.

Dès lors, la demande de caméras équipées de la technologie de reconnaissance faciale dans les magasins devrait augmenter au cours de la période de prévision. Outre la sécurité et la surveillance, la demande de technologie dans l'industrie est alimentée par l'application croissante de l'amélioration des connaissances des consommateurs pour offrir une meilleure expérience client.

Par exemple, la technologie pourrait être utilisée pour identifier un client dès son entrée dans le magasin, puis afficher des recommandations ou des offres personnalisées sur des écrans numériques dans tout le magasin.

De plus, recevoir des mises à jour sur les données démographiques réelles des clients visitant le magasin à un moment donné peut constituer un défi majeur pour toute direction de magasin de détail. La mise en œuvre de la technologie de reconnaissance faciale peut aider les autorités des magasins à accéder aux données démographiques de la fréquentation entrant dans le magasin toutes les heures et à prendre des décisions commerciales sur cette base.

La région Asie-Pacifique devrait enregistrer la croissance la plus rapide

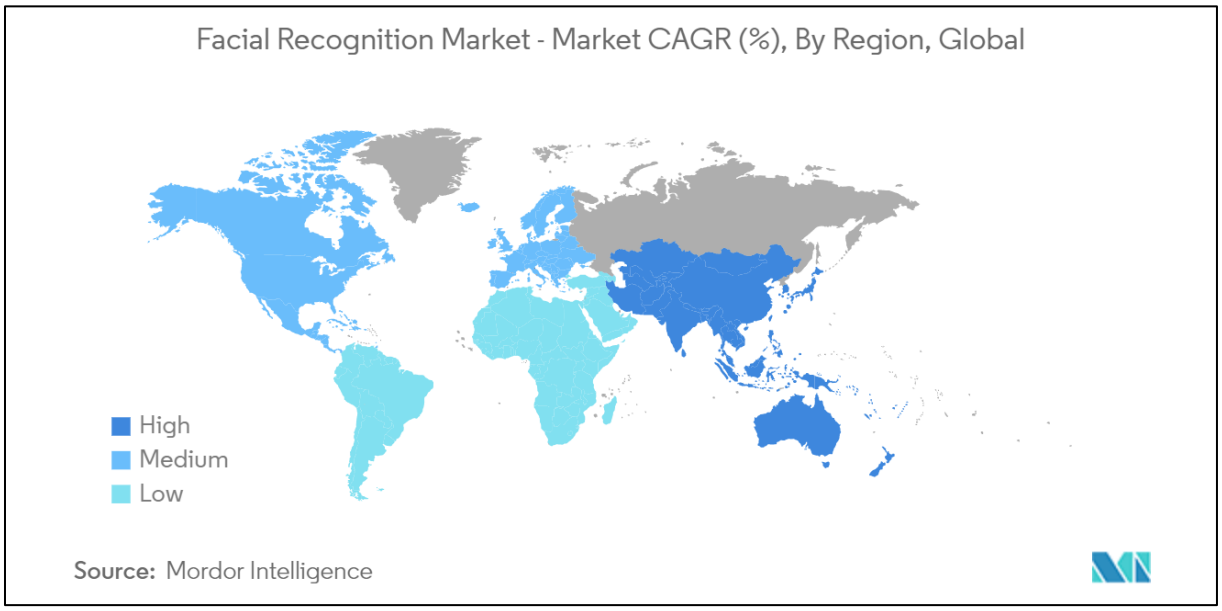
La région Asie-Pacifique est l' une des régions les plus en vue pour l' adoption de la reconnaissance faciale, en raison du développement technologique, de la croissance croissante des infrastructures et de l' application croissante dans de nombreux domaines. L' industrialisation massive et l' industrie croissante de l' électronique grand public dans la région présentent des opportunités passionnantes pour les acteurs du marché et la possibilité d' une croissance significative.

Ces dernières années, le secteur de la vente au détail en Inde est devenu de plus en plus dynamique et rapide, en raison de l'arrivée de nombreux nouveaux acteurs. L'industrie représente plus de 10 % du produit intérieur brut (PIB) du pays et environ 8 % de l'emploi (selon l'IBEF). Ainsi, le secteur de la vente au détail en expansion dans la région offre des opportunités de croissance considérables pour le marché.

De plus, en août 2022, l' aéroport international d' Hyderabad a annoncé l' utilisation de la reconnaissance faciale pour permettre des voyages fluides et sans tracas. Conformément au programme DigiYatra, l'aéroport international d'Hyderabad a déployé le traitement numérique des passagers comme preuve de concept via la plateforme DigiYatra.

La Chine utilise depuis longtemps la technologie de reconnaissance faciale. De plus, le pays a déployé des lunettes de reconnaissance faciale pour les forces de police du pays afin de repérer les citoyens et les touristes et d'utiliser l'authentification d'identité en temps réel pour lutter principalement contre les délits lors des célébrations.

Le pays adopte également les paiements authentifiés par reconnaissance faciale. Alipay, la plus grande application de paiement de Chine, a lancé un essai de la fonction smile-to-pay dans une succursale de KFC (Kentucky Fried Chicken) dans le sud de la Chine, qui utilise la reconnaissance faciale pour identifier les clients et les facturer automatiquement via l'application.



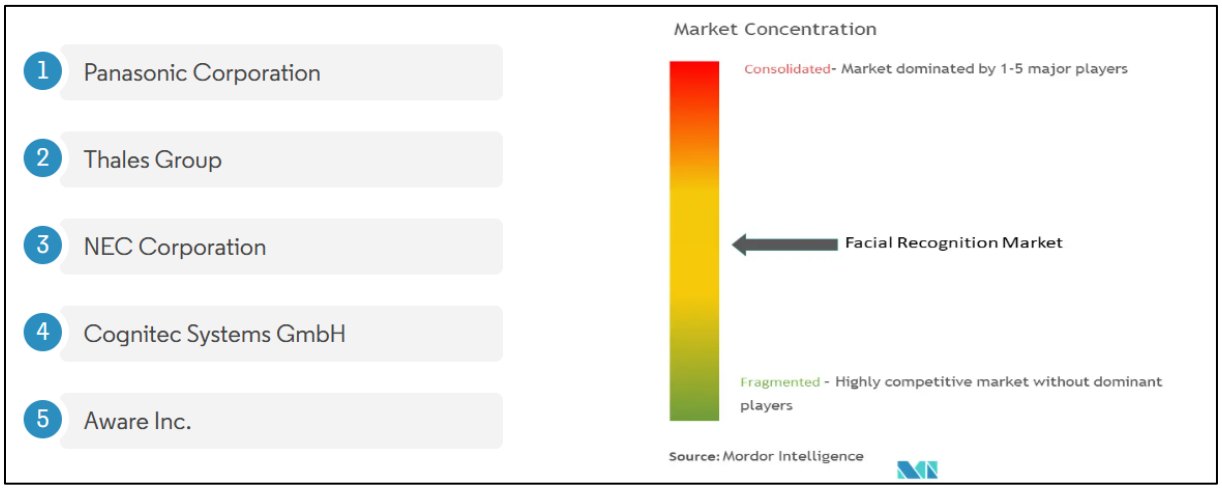
B. Aperçu du secteur de la reconnaissance faciale

Le marché de la reconnaissance faciale est modérément concurrentiel, avec des acteurs importants opérant sur le marché, tels que NEC Corporation, Gemalto NV, Panasonic Corporation, etc. Avec la croissance substantielle du nombre de startups, le marché étudié devrait bientôt connaître un scénario hautement concurrentiel.

En juin 2023, Hitachi, Ltd. et Panasonic Connect Co., Ltd. ont collaboré pour développer un nouveau service qui combine la technologie d'Hitachi pour prévenir les fuites de données biométriques avec la technologie de reconnaissance faciale de Panasonic Connect.

En novembre 2022, NEC Corporation a développé un système de contrôle d'accès sans porte utilisant la reconnaissance biométrique qui combine la technologie de reconnaissance faciale de NEC avec la technologie de réidentification des personnes, qui correspond aux personnes même si elles sont tournées vers l'extérieur ou si leur corps est masqué, pour fournir un contrôle d'entrée rapide et fiable. qui est libre de portes.

C. Les leaders du marché mondial de la reconnaissance faciale



Conclusion

Il s'avère que le sujet de la reconnaissance faciale est très controversé en raison du fait qu'il provoque de vifs débats dans le monde entier. Ainsi, si cette technologie est perçue comme étant très efficace par celles et ceux qui la plébiscitent pour sa rapidité et son objectivité dans l'accomplissement de ses missions, elle suscite de nombreuses inquiétudes en raison de ses imprécisions et biais qui peuvent entraîner des discriminations et porter atteinte à des droits fondamentaux, tels que notre liberté de manifestation.

Pourtant, cette note d'analyse a démontré que la reconnaissance faciale pouvait offrir de nombreux avantages, au quotidien.

Ainsi, manifester une opposition de principe à l'usage de la reconnaissance faciale serait faire preuve d'un manque de nuance évident. C'est pourquoi il pourrait être envisagé de légaliser l'usage de la reconnaissance faciale dans le strict respect du cadre légal défini par l'Union européenne. Pour légaliser la reconnaissance faciale en Belgique tout en respectant le cadre légal imposé par l'Union européenne (UE), il est essentiel de se conformer à plusieurs règles, notamment le Règlement général sur la protection des données (RGPD) et les principes des droits fondamentaux garantis par la Charte des droits fondamentaux de l'UE. Voici les conditions liminaires à remplir :

1° Évaluer les bases légales

La reconnaissance faciale implique un traitement de données biométriques, qui sont considérées comme des données sensibles selon le RGPD. Pour être légale, elle doit répondre à une base légale solide, comme :

- Consentement explicite : Les individus doivent donner leur consentement libre, éclairé et explicite. Quid des criminels et/ou des terroristes ?
- Intérêt public majeur : Cela peut inclure la sécurité publique ou la prévention de crimes graves, mais doit être prévu par une loi nationale spécifique.

- Exécution d'une mission d'intérêt général : Par exemple, dans le cadre d'un contrôle d'accès dans des lieux hautement sensibles (aéroports, centrales électriques, etc.).

2° Adopter une loi spécifique

La Belgique doit adopter une loi nationale qui encadre explicitement la reconnaissance faciale. Cette loi doit :

- Définir précisément les finalités pour lesquelles la reconnaissance faciale peut être utilisée (par exemple, contrôle frontalier, enquêtes judiciaires, etc.).
- Établir des garanties strictes pour prévenir les abus.
- Assurer une évaluation régulière de la proportionnalité et de la nécessité des mesures.
- Prévoir des mesures correctrices (droits de recours, destruction des données non nécessaires, etc.).

3° Assurer la proportionnalité et la nécessité

La reconnaissance faciale ne peut être déployée que si elle est :

- Nécessaire : Aucun autre moyen moins intrusif ne permet d'atteindre les objectifs fixés.
- Proportionnée : Les bénéfices (sécurité, efficacité) doivent être supérieurs aux atteintes potentielles aux droits fondamentaux.

4° Respecter les droits des individus

Conformément au RGPD et à la Charte des droits fondamentaux, il faut garantir :

- Transparence : Informer les citoyens sur l'utilisation de la reconnaissance faciale.
- Droits d'accès et d'opposition : Permettre aux individus de consulter les données les concernant et, dans certains cas, de s'opposer à leur traitement.
- Protection des données : Collecter uniquement les données strictement nécessaires et les stocker de manière sécurisée.

5° Consultation de l'Autorité de protection des données (APD)

L'APD belge doit être consultée lors de l'élaboration et de la mise en œuvre de la loi. Elle vérifiera que les principes du RGPD et les droits des citoyens sont respectés.

6° Limiter l'utilisation de la reconnaissance faciale dans l'espace public

Pour éviter des atteintes massives à la vie privée, des règles claires doivent être établies pour son utilisation dans les lieux publics, en limitant :

- Les zones concernées.
- La durée d'utilisation.
- Le croisement avec d'autres bases de données.

7° Encadrer les acteurs privés

Si la reconnaissance faciale est utilisée par des acteurs privés (centres commerciaux, stades, etc.), il est crucial de définir des règles spécifiques pour éviter une surveillance généralisée.

8° Assurer un contrôle indépendant

La mise en place d'un mécanisme de contrôle, par exemple par une commission indépendante ou l'APD (Autorité de protection des données), est essentielle pour :

- Surveiller le respect des lois et du RGPD.
- Enquêter sur les abus éventuels.
- Garantir des sanctions efficaces en cas de non-conformité.

9° Prévoir une période d'expérimentation

Une période d'expérimentation peut être instaurée sous supervision stricte pour tester la technologie et ses impacts avant une mise en œuvre à grande échelle.

10° Alignement avec les développements européens

La Belgique devra veiller à ce que sa législation nationale sur la reconnaissance faciale soit conforme aux exigences du règlement sur l'intelligence artificielle (AI Act), qui entrera en application progressivement à partir du 2 août 2026 et jusqu'en 2027 .

En résumé, la légalisation de la reconnaissance faciale en Belgique nécessite une approche équilibrée et rigoureuse, qui respecte les exigences de transparence, de proportionnalité et de respect des droits fondamentaux. Une consultation étroite avec les citoyens, les experts juridiques, les régulateurs et les institutions européennes est également essentielle pour assurer l'acceptabilité sociale et juridique.

Bibliographie

- https://www.europarl.europa.eu/thinktank/fr/document/EPRS_IDA(2021)698021

- https://www.europarl.europa.eu/news/fr/press-room/20240308IPR19015/intelligence-artificielle-les-deputes-adoptent-une-legislation-historique

- https://rm.coe.int/lines-directrices-reconnaissance-faciale-web-a5-2761-5835-0340-v-1/1680a31752

- https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_FR.pdf

- https://www.euractiv.fr/section/economie/news/les-technologies-de-reconnaissance-faciale-sont-deja-utilisees-dans-11-pays-de-lunion-europeenne-selon-un-rapport/

- https://www.rtbf.be/article/dans-les-rues-de-londres-la-police-utilise-desormais-la-reconnaissance-faciale-qu-en-est-il-en-belgique-11359230

- https://auvio.rtbf.be/media/reconnaissance-faciale-la-fin-de-l-anonymat-en-rue-3016338

- https://www.mordorintelligence.com/fr/industry-reports/facial-recognition-market

- https://www.autoriteprotectiondonnees.be/professionnel/themes/le-droit-a-l-image/reconnaissance-faciale-et-droit-a-l-image

- Entretien du 21 mai 2024 avec Rémy Farge, formateur à la Ligue des droits humain, à propos de la reconnaissance faciale.