LA RECONNAISSANCE FACIALE

UNE TECHNOLOGIE SENSIBLE ET PROMETTEUSE

Wixalia

SOMMAIRE

La reconnaissance faciale éthique est au service de la société

L’histoire se passe en Espagne, dans le cadre d’un test de la technologie de reconnaissance faciale par la police. Cela faisait dix ans que des enquêteurs travaillaient sur un enlèvement d’enfant. Ayant épuisé toutes les pistes, ils ne parvenaient toujours pas à retrouver le petit. Ils disposaient toutefois d’une piste sérieuse : ils avaient rassemblé assez d’indices pour localiser le périmètre éventuel où vivrait l’enfant. Et c’est en désespoir de cause que les enquêteurs ont décidé de recourir à la technologie de reconnaissance faciale pour quadriller le quartier et tenter de clore une bonne fois pour toutes cette affaire. Les enquêteurs ont donc installé des caméras avec un logiciel de reconnaissance faciale dans les endroits stratégiques du quartier où ils soupçonnaient que l’enfant, à présent adolescent, vivait. Au bout de huit jours, le système a détecté la présence de l’adolescent, et il fut rendu à sa famille.

De l’usage classique qu’on lui connait…

S’il fallait un seul argument pour convaincre de **l’utilité de la reconnaissance faciale,** ce serait ce cas, devenu emblématique. Une **affaire qui s’est bien terminée et dans laquelle la reconnaissance faciale**, même utilisée dans des conditions difficiles, car il fallait utiliser des photos de l’enfant à l’époque de sa disparition, dix ans plus tôt, **a montré toute son utilité** dans une dramatique affaire familiale. Car même si la reconnaissance faciale est devenue **l’une des technologies d’authentification biométrique les plus importantes** de ces dernières années, elle traîne dans son sillage beaucoup de malentendus et de controverses. Dans un contexte de défiance envers l’autorité, et de craintes pour la préservation de la vie privée, les entreprises hésitent. IBM, AWS et Microsoft ont annoncé qu’ils ne mettront pas à la disposition de la police leurs technologies de reconnaissance faciale. Cependant, même s’ils semblent apporter de l’eau au moulin des détracteurs de la reconnaissance faciale, ces géants de la Tech ne ferment pas la porte à l’usage de leurs technologies par les gouvernements. Ils reconnaissent son utilité dans beaucoup de cas d’usage et demandent **un cadre légal qui protège les libertés et sauvegarde la vie privée des personnes**. « Nous ne vendrons pas la technologie de reconnaissance faciale aux services de police des États-Unis tant que nous n’aurons pas une loi nationale, fondée sur les droits de l’homme, qui régira cette technologie », a déclaré Brad Smith, président de Microsoft, lors d’une interview au Washington Post.

… à des cas d’usage polyvalents

Malgré ces prises de position, la **reconnaissance faciale** est une technologie qui s’est avérée **suffisamment polyvalente pour être déployée** dans bien des domaines. D’après une étude publiée par le cabinet de recherche Research AndMarkets, La **taille du marché mondial de la reconnaissance faciale devrait atteindre 9,93 milliards de dollars d’ici 2027.** Un marché devrait se développer à un **taux de croissance annuel moyen de 14,5 %** entre 2020 et 2027. Selon le cabinet, les avancées technologiques telles que les systèmes de reconnaissance 3D et les solutions basées sur le cloud et une adoption croissante de la reconnaissance dans diférents secteurs verticaux **constitueront les principaux moteurs du marché.**

La reconnaissance faciale fait son chemin auprès du grand public dans les grands événements planétaires. Les organisateurs des Jeux olympiques de Tokyo vont la déployer afin d’assurer la sécurité des athlètes, du staff, des journalistes et des bénévoles. En France, **la CNIL, pourtant très regardante sur les conditions d’attribution des autorisations, aurait donné son feu vert** pour des expérimentations en vue d’un déploiement à grande échelle durant les JO de Paris en 2024. L’objectif est de proposer aux spectateurs qui le veulent de passer par des portiques avec reconnaissance faciale pour rendre les entrées plus fluides.

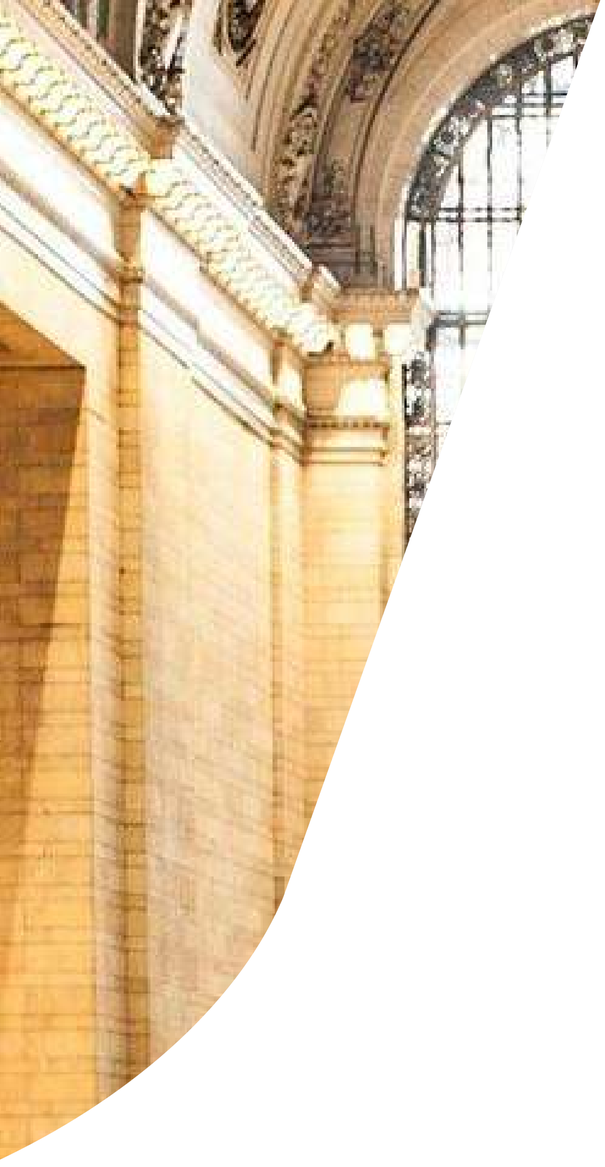
Une démarche structurante dans le cadre d'une stratégie à long terme

Bien qu'il existe des méthodes fiables d'identification biométrique, telle que la numérisation des empreintes digitales et de l'iris, la reconnaissance faciale s'avère efficace et conforme aux règles de distanciation physique. Le système n'exige rien de ses utilisateurs, il est sans contact. En outre, la technologie a connu une propagation généralisée auprès du grand public à travers les smartphones. **La maturité de la technologie à des prix compétitifs contribue grandement à l'émergence de la reconnaissance faciale**, et à la généralisation des cas d'usage comme nous le verrons dans ce Livre Blanc.

Pour l'entreprise qui voudrait déployer la technologie de reconnaissance faciale, son intégration dans une démarche stratégique à long terme est nécessaire. C'est une démarche structurante qui exige une réflexion approfondie, une planification minutieuse et une exécution rigoureuse des différentes étapes de déploiement. Elle doit s'intégrer dans des modèles commerciaux et sécuritaires appropriés et conformes au respect des réglementations en vigueur. Dans ce contexte, l'intervention d'un intégrateur s'avère incontournable, car il apporte son expérience des cas d'usages ainsi qu'une connaissance pratique des écueils et obstacles à surmonter, qu'ils soient techniques ou juridiques.

Il s'agit concrètement de **mettre en place une infrastructure sécurisée** de collecte, de stockage et de traitement des données, les technologies du Big data en somme. Ce qui nécessite le **déploiement de technologies de pointe comme les bases de données, l'intelligence artificielle et un réseau de transport performant et sécurisé**. Ces prérequis sont plus faciles à mettre en œuvre qu'il peut sembler à priori et font de la reconnaissance faciale un formidable accélérateur de transformation numérique.

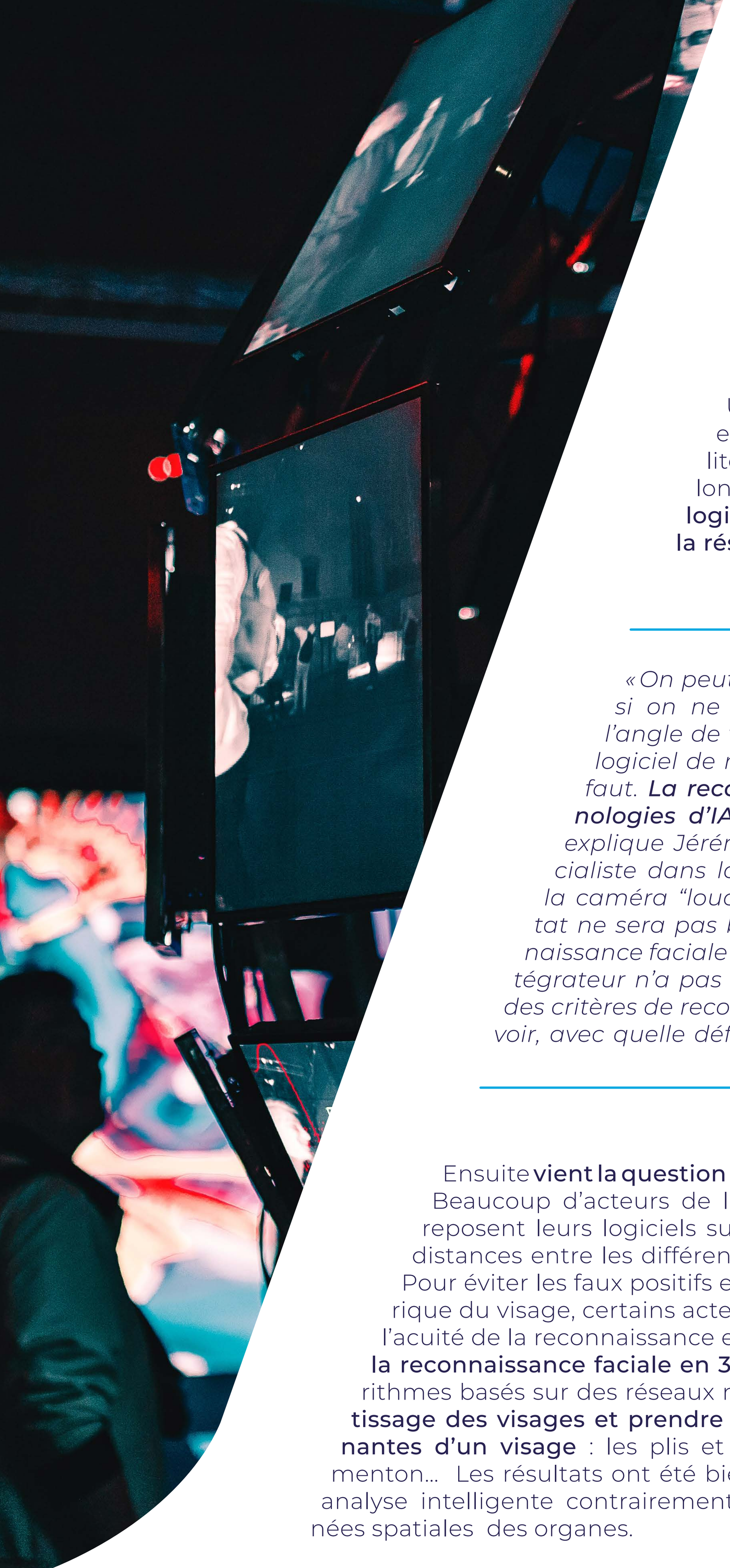
« Tous les systèmes de reconnaissance faciale fonctionnent sur le principe de conversion de données spatiales en formules mathématiques. Ce transcodage des informations graphiques en informations mathématiques offre sécurité et conformité, puisque les formules mathématiques qui modélisent le visage ne peuvent pas être rétroconverties en images ».



Comment fonctionne la technologie de reconnaissance faciale ?

La technologie de reconnaissance faciale permet l'identification d'une personne ou d'un objet par la mise en correspondance de caractéristiques physiques de référence stockées, comparées avec des caractéristiques dans les images prises en direct. Pour ce faire, elle détecte et mesure diverses coordonnées faciales. Cependant, et contrairement à une idée tenace et encore trop répandue, **les images de référence ne sont pas stockées telles quelles dans les systèmes de reconnaissance faciale.** Pour économiser l'espace de stockage et accélérer la reconnaissance, les données remontées par le système sont des métadonnées : **les portraits sont remplacés par des modèles mathématiques. C'est-à-dire que les images capturées sont converties en une représentation numérique** qui reprend les principales caractéristiques du visage d'un individu : la forme du visage et des organes (yeux, nez…), les distances entre ces différents organes comme l'écartement des yeux, les courbes d'implantation des cheveux, les oreilles…

Tous les systèmes de reconnaissance faciale fonctionnent sur ce principe de conversion de données spatiales en formules mathématiques. Ce transcodage des informations graphiques en informations mathématiques présente plusieurs avantages. Il permet de **préserver la correspondance même si les caractéristiques faciales varient légèrement, comme lors de la prise de poids ou du vieillissement**. Il offre aussi plus de sécurité, puisque les formules mathématiques qui modélisent le visage ne peuvent pas être rétroconverties en images. De plus, **si le système est piraté, les données ne pourront pas être lues et encore moins utilisées par un autre système.** Seul le système qui a créé le modèle mathématique est capable de le lire.



Acuité de la reconnaissance et différences entre algorithmes 2D et 3D

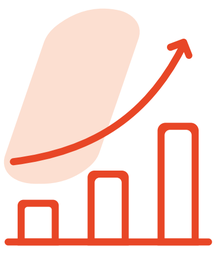
Un système de reconnaissance faciale est une chaîne de traitement dont la qualité globale repose sur les différents maillons qui la composent. **La base d'un bon logiciel de reconnaissance faciale reste la résolution de la caméra.**

« On peut avoir le meilleur logiciel du monde, mais si on ne dispose pas d'une définition suffisante, l'angle de vue suffisant et le bon positionnement, le logiciel de reconnaissance faciale va être mis en défaut. ***La reconnaissance faciale fait partie des technologies d'IA qui repose sur ce que voit le logiciel,*** *explique Jérémie Caron, Consultant de Wixalia et spécialiste dans la sécurité des personnes et des biens. Si la caméra "louche" ou souffre d'un "strabisme", le résultat ne sera pas bon. Nous avons vu des projets de reconnaissance faciale qui tombaient à l'eau, juste parce que l'intégrateur n'a pas bien fait son travail dans la qualification des critères de reconnaissance, tel que qu'est-ce qu'on devait voir, avec quelle définition et quelle est la finalité derrière ? ».*

Ensuite **vient la question de l'algorithme sur lequel repose l'analyse.** Beaucoup d'acteurs de l'algorithmie de la reconnaissance faciale reposent leurs logiciels sur de la 2D, c'est-à-dire sur la mesure des distances entre les différents organes du visage (nez, yeux, oreilles…). Pour éviter les faux positifs en prenant une véritable empreinte numérique du visage, certains acteurs du marché ont voulu pousser plus loin l'acuité de la reconnaissance en prenant en compte plus de détails, c'est **la reconnaissance faciale en 3D.** Pour ce faire, ils ont introduit des algorithmes basés sur des réseaux neuronaux pour faire **un véritable apprentissage des visages et prendre en compte toutes les aspérités discriminantes d'un visage** : les plis et les rides, la calvitie ou pas, la forme du menton… Les résultats ont été bien plus proches de ce qu'on attend d'une analyse intelligente contrairement au simple enregistrement de coordonnées spatiales des organes.

La reconnaissance faciale en 3D identifie et analyse les différentes caractéristiques d'un visage humain, qui sont toutes uniques et ne changent pas avec le temps. En outre, elle présente des avantages par rapport à la reconnaissance faciale 2D, comme la **facilité de détection des données faciales à partir de vidéos et d'images 2D** et le fait qu'elle soit moins affectée par les problèmes d'éclairage. Avec le développement des logiciels et des services de reconnaissance faciale en 3D, la mise en œuvre de la reconnaissance faciale se développe, notamment dans les secteurs des solutions informatiques pour les soins de santé, des paiements et du commerce.

+35%



« Grâce à la 3D, nous sommes passés d'un taux de reconnaissance d'environ 60 % il y a quatre à cinq ans, pour atteindre aujourd'hui, si les spécifications de qualité sont bien respectées, ***des taux supérieurs à 95 %*** *» souligne Jérémie Caron.*

« En fin de compte, c'est la qualité et la précision de la qualification du projet par l'intégrateur en amont qui fera la réussite du projet ou son échec. C'est la clé pour qu'un déploiement se passe bien ».

Jérémie Caron Consultant de Wixalia et spécialiste dans la sécurité des personnes et des biens.

Un partenariat technologique et réglementaire avec l'intégrateur

Comme toute technologie qui repose sur une chaîne complexe de collecte, de traitement et de stockage de données, **la reconnaissance faciale repose sur les mêmes principes que la mise en place d'un système de Big data et d'intelligence artificielle.** Sa précision est fortement dépendante de la qualité des données utilisées; ce qui place la qualité des normes et moyens de collecte des données, la qualité de l'image par exemple, en premier dans la chaîne de traitement. Sur un marché où divers acteurs se positionnent, c'est ce qui fait la différence entre un intégrateur et un installateur.

*« C'est la raison pour laquelle **on parle bien d'intégrateur et pas d'installateur.** Un installateur, comme son nom l'indique, installe du matériel. Il travaille plutôt en mode boite noire et ne vend pas une solution vidéo, mais un "magnétoscope", en somme un prix dans la plupart des cas. **Un intégrateur doit pouvoir proposer plusieurs services** : une branche installation et une autre d'intégration et de mise en service ».*

Le déploiement d'une solution de reconnaissance faciale fait ainsi appel à de larges compétences techniques et place l'intégrateur dans un rôle où la **maîtrise des produits de capture d'image et des technologies applicatives et réseau sont primordiaux.**

« ***Un bon intégrateur est constamment en veille technologique, en formation et en suivi des nouveaux produits,*** *pour proposer les meilleurs matériels à ses clients. C'est ce qui fait la différence entre un intégrateur à valeur ajoutée et un intégrateur-installateur* », affirme Jérémie Caron.

Une bonne qualification du projet est essentielle

Comme toute technologie qui repose sur une chaîne complexe de collecte, de traitement et de stockage de données, la reconnaissance faciale repose sur les mêmes principes que la mise en place d'un système de Big data et d'intelligence artificielle. **Pour l'entreprise, elle s'apparente à une transformation numérique nécessitant la mise en place d'une infrastructure sécurisée de collecte de stockage et de traitement de données.** La sécurisation et l'intégrité des données en transit et des points finaux, sont autant de défis qui doivent être adressés dès la conception du projet.

Mais pour que ce déploiement soit un succès, ***une bonne définition des besoins en fonction des cas d'usage*** *est une étape où le choix du prestataire est primordial, car, « en fin de compte, c'est la qualité et la précision de la qualification du projet par l'intégrateur en amont qui fera la réussite du projet ou son échec. C'est la clé pour qu'un déploiement se passe bien »,* insiste Jérémie Caron.

Une approche de transformation numérique dans laquelle l'intégrateur apporte son savoir-faire à toutes les étapes :

1. La mise en place d'une stratégie globale,
2. l'idéation d'un ou plusieurs cas d'utilisation et du prototypage d'un POC,
3. la conception de la plateforme ainsi que la connexion des appareils et des objets,
4. l'adaptation des SI existants et leur intégration dans un système plus global.

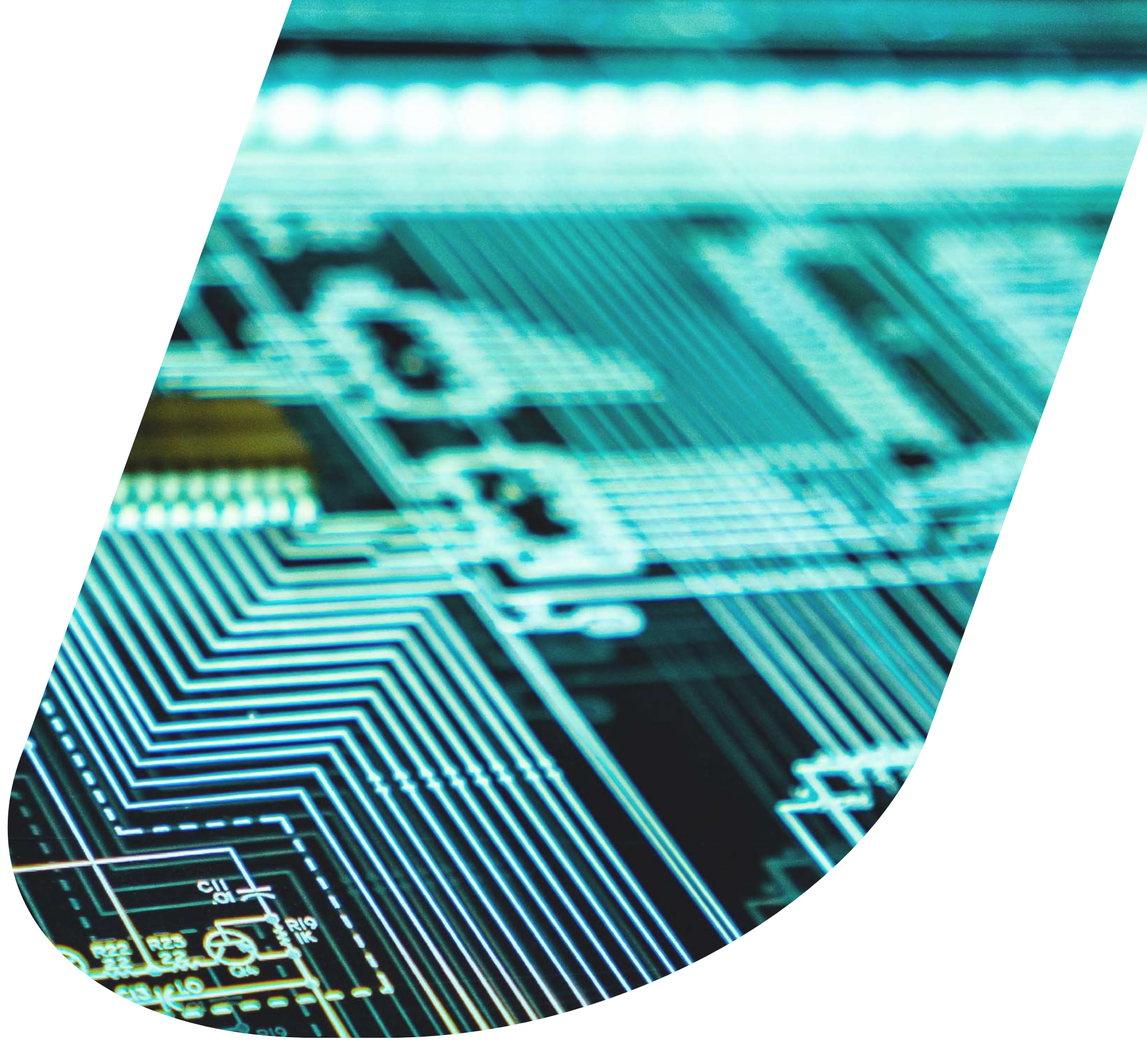
Mettre en place une plateforme sécurisée

Par exemple, concernant la sécurité des données transitant dans le réseau, **le chiffrement de bout en bout est la solution la plus efficace,**

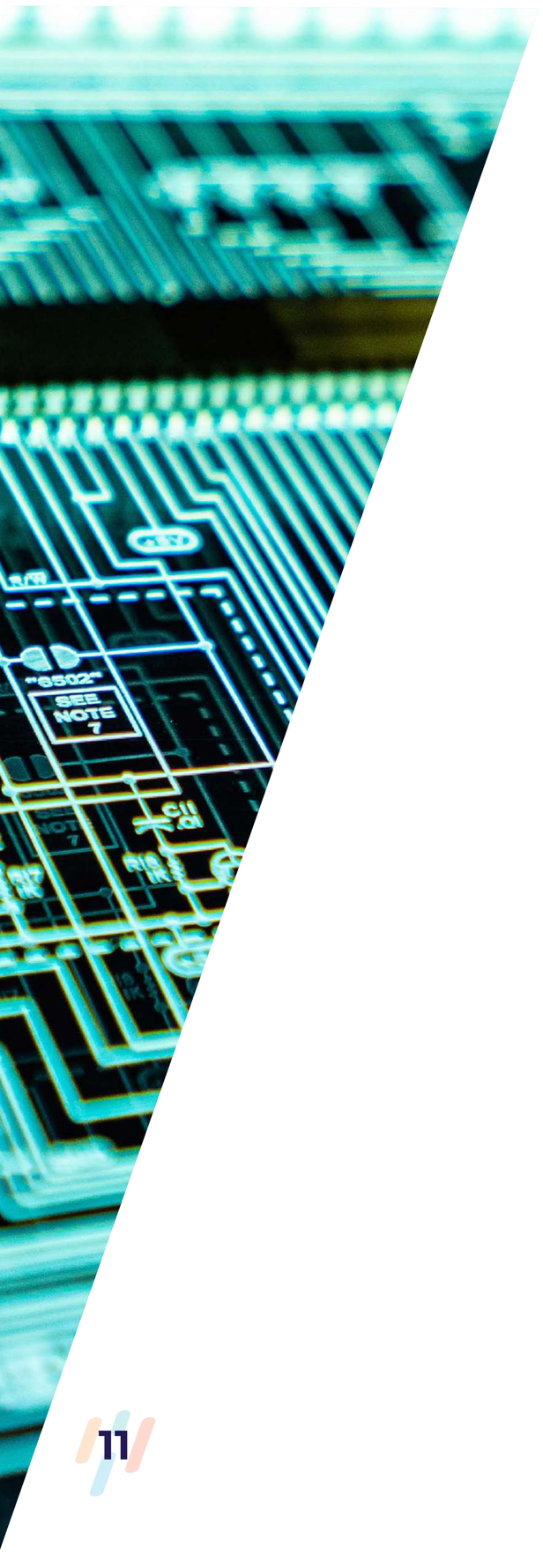
---

*« mais **il y a très peu d'intégrateurs qui savent le faire**, ce qui élimine une bonne partie des intégrateurs qui opèrent sur ce marché,* révèle Jérémie Caron. *Un bon intégrateur doit être capable d'étanchéifier le réseau, chiffrer les communications de bout en bout, assurer la sécurité par des dispositifs comme le firewalling, et, pourquoi pas, compléter avec de l'analyse de protocoles et d'applications selon le niveau de sécurité désiré ».*

Enfin, l'entreprise doit avoir une bonne compréhension de ce qu'implique un projet de reconnaissance faciale sur son SI, ses processus et de la conformité à la



réglementation. La plupart des entreprises utilisent encore des systèmes informatiques hérités, qui n'ont pas été conçus pour traiter un tel cas d'usage. C'est pourquoi **les conseils et l'intervention d'un intégrateur ayant les compétences et l'expérience nécessaires** pour mettre en place ces plateformes intelligentes et sécurisées sont essentiels.



Cas d’usage et implémentation de la reconnaissance faciale

La législation actuelle ne permet pas la mise en œuvre de beaucoup de cas d’usage, ceci même si la technologie de reconnaissance faciale présente une solution efficace à un problème. Influencée par les premiers usages implémentés, comme les cabines de contrôle aux frontières dans les aéroports, **la reconnaissance faciale est trop souvent identifiée à la sécurité, mais son champ d’application est bien plus large.** Elle présente des avantages certains dans le cadre de l’évolution sociétale post-Covid-19, où le principe de précaution, et la crainte d’un retour de la pandémie favorisent la société sans contact.

*« La crise du Covid-19 a fait émerger des cas d’usage qui ont fait comprendre que l’**on peut faire beaucoup de choses positives avec la reconnaissance faciale**. Le but de la reconnaissance faciale n’est pas seulement de rechercher des brigands ou des terroristes, on peut aussi, grâce à cette technologie, protéger les individus dans leur vie quotidienne ».* explique Eli Goldmann, directeur du Business développement chez Wixalia.

Dans beaucoup de cas, la législation devra évoluer pour ouvrir certains champs d’application de la reconnaissance faciale. Cependant, lorsque toutes les conditions réglementaires sont réunies, en France la CNIL peut délivrer des autorisations pour des déploiements spécifiques.

Contrôle des accès et sécurité

Les deux cas concrets décrits ci-dessous sont réels et illustrent la puissance de la reconnaissance faciale quand celle-ci est couplée à l'intelligence artificielle. Comme nous le verrons, les bénéfices obtenus vont bien plus loin que ceux que l'on attend d'un « simple » contrôle d'accès.

Cas n°1 / Hôpital spécialisé : protection humaine (des infirmiers et soignants) et protection de personnes vulnérables d'elles-mêmes.

D'après les prévisions des cabinets d'étude, la reconnaissance faciale dans le segment des soins de santé devrait connaître le plus fort taux de croissance dans les prochaines années. Son utilité va bien au-delà de la sécurisation des accès ou la restriction des accès aux zones sensibles, comme les zones de stockage de médicaments (pour éviter les vols de matériel et de médicaments par exemple). Elle est aussi utile dans le cas de la prévention de la transmission de maladies, au premier chef desquels la Covid-19, mais aussi dans plusieurs cas d'usage, comme la régulation des visites aux malades ou l'identification des patients pour accéder à leur dossier médical.

L'une des implémentations dans le domaine de la santé réalisée par Wixalia a concerné la sécurité humaine au sens de protection de la personne, pas des agressions, mais d'elle-même. L'hôpital spécialisé client, situé à l'étranger, voulait s'assurer que seules les personnes autorisées dans un service de psychiatrie, puissent accéder à certaines zones. Les responsables de la sécurité se sont aperçus que certains patients étaient capables de voler un badge à un soignant pour ouvrir des portes qui autrement leur seraient fermées. Leur objectif était de décourager les patients fugueurs ou d'interdire l'accès aux locaux contenant des médicaments, notamment des seringues et des narcotiques.

Avec la solution de reconnaissance faciale, **même si le patient vole un badge, il ne pourra pas tromper le système de sécurité**. « *Il pourra voler le badge, mais pas le visage de la personne à laquelle il appartient* », ironise le responsable du projet. Après un audit de l'infrastructure de l'hôpital, qui disposait déjà d'un réseau de caméra plutôt récent, il a été décidé de s'appuyer sur cette infrastructure existante. Il a juste suffi de régler les champs de vision couverts par les caméras, pour les optimiser pour la reconnaissance faciale. Une fois le système mis en production, l'hôpital a voulu étudier la possibilité d'aller plus loin en utilisant **l'intelligence artificielle, cette fois pour protéger les patients et le personnel en cas de problème.**

Protéger les patients et les soignants

Il s'agissait de déployer des fonctions de protection des patients et des soignants dans les lieux où ils pourraient se retrouver isolés. Il a ainsi été procédé aux tests pour détecter les chutes de personnes pour intervenir dans les cas de crise, ou d'agression d'un soignant par un patient instable.

Les techniciens ont également exploré d'autres scénarios pour détecter les anomalies, voire les incidents. Notamment une fonction de reconnaissance d'uniformes pour vérifier si la personne filmée faisait partie de l'équipe soignante ou si c'était un patient, car les uniformes des uns et des autres sont de couleurs et de formes différentes. Ceci pour alerter le PC Sécurité, en cas d'anomalie, comme la présence d'un patient à un endroit où il n'est pas supposé être. Un des scénarios demandés par les responsables de l'hôpital consistait à détecter automatiquement des incidents pour en alerter la sécurité, comme par exemple un aide-soignant à terre entouré de patients.

Ces explorations permettaient à la sécurité de l'hôpital de mettre en place les processus de réponse aux incidents. Les protocoles d'intervention lorsqu'un patient est au sol ou lorsqu'un soignant est au sol sont différents. Dans le premier cas, il s'agit généralement de pathologie où le patient est en crise, dans le second c'est traité comme un incident et c'est la sécurité qui intervient.

Cas n°2 / Caserne : s'assurer qu'aucune personne non habilitée ne pénètre dans une zone classifiée.

À première vue, l'intitulé de ce cas client peut s'apparenter à un simple contrôle d'accès, mais il n'en est rien, car le système de reconnaissance faciale déployé dans cette caserne permet un contrôle beaucoup plus fin des accès. Il prend en compte la qualité (un gradé par exemple) de la personne qui rentre dans la caserne et les endroits qui lui sont accessibles ou pas. Il est inspiré des systèmes que l'on rencontre dans les aéroports : les personnes qui rentrent dans la caserne sont photographiées lorsqu'elles passent leurs badges à l'entrée et sont automatiquement enrôlées dans le système.

Les zones à laquelle est habilitée la personne sont définies à ce stade en fonction du badge qu'elles ont passé dans le lecteur. Le défi que présentait ce système de reconnaissance faciale est qu'il fallait mettre en place un réseau de caméras qui permette de couvrir des champs visuels assez serrés pour plus de précision, ainsi qu'un réseau de radars de détection de présence. Les techniciens ont ainsi déployé deux types de caméras : des modèles contextuels à champ large et des modèles aux angles de prise de vue plus resserrés.

Lorsqu'un radar détecte une présence, il envoie les coordonnées géographiques à la caméra motorisée à longue focale, qui panote et zoome sur l'individu afin de s'assurer de son identité et de ses habilitations. Pour obtenir cette coordination, les techniciens ont établi des cartographies des zones à surveiller, puis les ont géocodées, avec des matrices de distances, afin de synchroniser les références spatiales entre les radars et les caméras. Le système s'est avéré efficace et, comme dans le cas de l'hôpital ci-dessus, une extension des cas d'usages est envisagée.

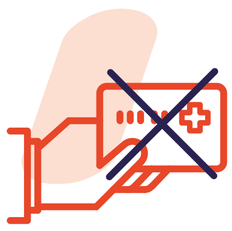
Les autres champs d'application de la reconnaissance faciale

Si aujourd'hui la reconnaissance faciale dans ses applications les plus connues reste l'apanage de la sécurité et le contrôle des accès, de nombreux autres cas d'usages sont déployés sans qu'ils fassent la une des journaux. Il est également intéressant de se projeter dans un avenir encadré par une nouvelle règlementation et de découvrir des cas d'usage très prometteurs.

Le secteur de la Santé

Nous l’avons vu plus haut, la reconnaissance faciale est une technologie pertinente pour la protection des personnes vulnérables et le contrôle pointu des accès. Mais pas que…

La crise sanitaire a mis en évidence le besoin de limiter au maximum le contact physique entre humains mais également avec des superficies susceptibles d’être contaminées. Ici aussi la reconnaissance faciale se positionne en un allié de choix pour mettre en place une stratégie de « non contact » dans un environnement sanitaire, car elle réduit de manière très efficace les risques de contagion :



Accès aux différentes zones d’un hôpital et en particulier aux blocs opératoires, sans besoin de badger ou de toucher des portes ou des points de contrôle.

Traçabilité des cas contacts au sein d’un hôpital lorsqu’un soignant est testé positif ou une personne malade est sortie de la zone de soin sans autorisation :

il est possible de retracer au sein de l’établissement sur une période définie les déplacements et les contacts d’un individu avec les autres et ainsi d’isoler seulement les vrais cas contacts.

D’autres projets e-santé basés sur l’identification par reconnaissance faciale sont également en cours d’étude, comme le développement d’un carnet de santé numérique dont l’accès est sécurisé par un profil biométrique. La protection des données personnelles de l’individu est renforcée par rapport à des empreintes digitales, et conformément aux règlementations internationales, seuls les éléments techniques de l’algorithme biométrique requis pour le fonctionnement de l’identification sont stockés.

Le secteur de la santé sera dans les années à venir porteur de nombreuses innovations liées à la reconnaissance faciale, notamment pour sa garantie des gestes barrière et sa fiabilité dans l’identification des individus.

Le commerce, les services et l'industrie

La reconnaissance faciale a également un avenir très prometteur au-delà des usages habituels de contrôle d'accès ou de sécurité publique et privée.
L'amélioration du service à la clientèle, l'analyse des comportements des acheteurs, les paiements sans friction ne sont que quelques-unes des applications qui sont apparues sur le marché ces dernières années.
L'analyse vidéo couplée à l'intelligence artificielle a un fort potentiel dans de nombreux secteurs.

On retiendra en particulier :

Dans le retail et le luxe

Tout spécialement, la personnalisation de la relation client grâce à l'identification des clients lors de leur arrivée en magasin, suppose une relation unique entre la cible et la marque.

Dans les centres commerciaux

Une combinaison de reconnaissance faciale et de Big Data permet de mettre en évidence les endroits les plus fréquentés (appelés points chauds), de visualiser les parcours client, suivre les arrêts devant les vitrines, etc. pour ensuite calculer la fréquentation et en déduire des modèles de parcours des visiteurs, Le tout mis en corrélation avec les dépenses effectuées, les endroits où elles ont été faites ou une analyse démographique de la clientèle. Rappelons que dans un système de ce type, aucune donnée personnelle n'est traitée. Les personnes sont identifiées par des étiquettes alphanumériques et suivies par le système afin de connaître certaines informations comme leurs parcours ou le temps de présence et les magasins visités par exemple.

Dans le transport de voyageurs

L'usage de la reconnaissance faciale permettrait de combattre la fraude et d'effectuer les contrôles sans contact à l'embarquement. Les utilisateurs ayant installé l'app du transporteur, ou accepté de se faire prendre en photo lors de l'achat de leur billet pourraient être contrôlés via la reconnaissance faciale. Le passage des points de contrôle s'effectuerait ainsi sans contact et resterait fluide.

Autre usage intéressant dans ce secteur est l'anticipation du volume des bagages dans les trains et les avions. La multiplication des bagages en cabine entraine régulièrement des retards de vols, donc des coûts pour les compagnies. Grâce à la reconnaissance des objets, les compagnies peuvent mesurer le volume de bagages en salle d'attente et inciter les voyageurs à les mettre en soute avant l'embarquement et éviter les retards.

Dans l'industrie et la logistique

La reconnaissance des objets présentent de nombreux avantages et les entreprises réfléchissent déjà à de nouvelles applications, comme contrôler la manipulation des matières dangereuses ou sensibles, retrouver des colis égarés, vérifier que les employés portent leurs équipements de protection tel un casque ou une combinaison, ou que certains engins ou machines sont utilisés par les personnes autorisées.

Dans le secteur de la Banque

Nombre d'entités ont déjà mis en place, ou y travaillent, l'identification des clients par reconnaissance faciale à partir d'un smartphone. Ce développement répond également à la directive européenne sur les services de paiement (DPS2) qui comprend entre autres l'obligation de l'authentification forte (c'est-à-dire à deux facteurs au moins entre un code ou mot de passe que l'on sait, un appareil que l'on possède, une donnée biométrique telle que l'empreinte digitale, la voix ou l'iris) pour les paiements en ligne de plus de 30 euros, afin de réduire la fraude dans l'e-commerce.

Ce ne sont là que quelques exemples, parmi tant d'autres que l'on pourrait citer. Certains existent déjà dans notre quotidien, d'autres sont de l'ordre de la réflexion et de l'anticipation. Le champ des possibles de la reconnaissance faciale n'a qu'une limite et on en comprend bien l'enjeu : la législation et la protection des libertés individuelles. Ainsi l'amorce d'une discussion entre les parties-prenantes (le légal, la technique et la société en général) semble nécessaire pour démystifier cette technologie et préparer un futur plus ouvert qui permettra cette diversification des usages.

« Il n'existe pas de cas de législation aussi restrictive que la législation européenne. ***Ceci est dû à un dialogue et une compréhension mutuelle complexes entre le réglementaire, la technique, et les personnes****. ».*

Victoria HAUSER, consultante spécialiste de la conformité et de la cybersécurité chez Synelience.

La réglementation, le respect des libertés et la protection des données personnelles

L'un des droits les plus fondamentaux dans les démocraties européennes est le droit à la liberté d'aller et venir anonymement et le droit à la vie privée. C'est la raison pour laquelle, la loi pose un principe d'interdiction de tout traitement de données biométriques aux fins d'identifier une personne physique de manière unique. Plusieurs textes, nationaux et européens réglementent les différents aspects de la collecte et du traitement des données personnelles :

la loi du 6 janvier 1978 dite Informatique et liberté,

modifiée par la loi du 20 juin 2018,

puis par l'Ordonnance du 12 décembre 2018 ;

le Règlement européen 2016/679 ou RGPD 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 ;

ainsi que la Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative au traitement des données en matière pénale dite Police Justice.

Le droit européen reconnaît comme « données sensibles » les images faciales des personnes. Elles font partie des données biométriques qui rentrent sous la juridiction des données personnelles au même titre que les informations d'état civil. **À ceci près que la réglementation en vigueur considère que les données biométriques sont plus « sensibles » que les données d'état civil et que leur sécurité doit être renforcée car leur mauvais usage peut porter une atteinte accrue à la vie privée des personnes concernées**. Cependant, s'il est difficile pour une personne mal intentionnée d'obtenir les dates de naissance de ses victimes potentielles, il est très facile de capturer des images des personnes ciblées dans les lieux publics.

Une démarche très encadrée

C'est la raison pour laquelle le législateur a voté un certain nombre de lois, dont la plus connue est le RGPD (Règlement général sur la protection des données), pour protéger les citoyens européens d'un usage abusif de leurs données personnelles, dont les données biométriques font partie. Selon Victoria HAUSER, consultante spécialiste de la conformité et de la cybersécurité chez Synelience, *« il n'existe pas de cas de législation aussi restrictive que la législation européenne*. ***Ceci est dû à un dialogue et une compréhension mutuelle complexes entre le réglementaire, la technique, et les personnes***. *»* . Et même si le principe d'interdiction s'applique d'emblée, la réglementation prévoit plusieurs cas dans lesquels ce traitement peut être entrepris :

Lorsque la personne concernée a donné son consentement mais cela implique qu'elle comprenne l'intérêt du traitement de ses données et qu'elle en conserve la maîtrise.

Lorsque le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail.

Lorsque le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement.

Lorsque le traitement est nécessaire pour des motifs d'intérêt public importants (art.9.2 du RGPD).

Les organismes, privés ou publics, qui souhaitent mettre en place un système de reconnaissance faciale doivent respecter la réglementation relative au traitement des données personnelles. Notamment les articles sur la constitution de fichiers de données personnelles et les délais de rétention de ces informations.

Ceci est conditionné à un contrôle strict des mesures de sécurité relatives à la vie privée des personnes. **C'est ce que l'on appelle le respect des principes de « privacy by design » et de « security by default ».** Ces derniers servent à mesurer les risques en amont et à les traiter en prévention d'un point de vue organisationnel, juridique et technique pour que le service soit conforme à sa sortie.

Ceci suppose également que les personnes soient informées clairement et explicitement du traitement qui est fait de leurs données (« Ce qui se conçoit bien s'énonce clairement…. »).

Suivant la réglementation, le responsable du traitement des données doit mener une étude d'impact sur la vie privée. **Il s'agit de s'assurer que le système de reconnaissance faciale mis en place ne déroge pas à la loi et n'engendre pas de risques pour les droits et les libertés des personnes physiques.** L'étude d'impact doit être ensuite adressée à la CNIL pour avis.

Pour les entreprises soucieuses de respecter le RGPD, la CNIL a mis en ligne un outil d'analyse, l'AIPD ou analyse d'impact relative à la protection des données, pour aider les responsables à construire des traitements de données respectueux de la vie privée, mais aussi à démontrer leur conformité aux lois en vigueur.

Le RGPD est une première convergence entre les textes et la réalité technologique. Certes avec une série d'exigences qui peuvent sembler beaucoup trop chronophage pour les entreprises souhaitant développer ce type de solutions, mais c'est un investissement initial qui est facilement amorti avec le temps, et qui n'en reste pas moins un bon garde-fou pour bien construire le projet et éviter toute dérive.

Conclusion

Les cas d'usage de la technologie de reconnaissance faciale concrets et bien explicités apportent des solutions que les autorités de régulation n'ont pas de raisons de refuser. Or, l'enjeu des technologies au XXIème siècle est bien celui-ci : **l'harmonisation des nouveaux usages basés sur la technologie avec les règles juridiques qui sont le fondement de la démocratie.** L'individu, quel qu'il soit, ayant compris que l'utilisation de ses données dans la poursuite d'un but utile et sans lui nuire ne sera pas enclin à refuser ce traitement.

La révolution numérique est bel et bien en marche, dans un contexte où **la technologie avance plus vite que la règlementation**. L'avenir et les nouveaux développements technologiques passeront par des solutions hybrides où la biométrie en général et la reconnaissance faciale (morphologique ou des objets) en particulier seront les nouveaux accélérateurs de transformation des entreprises.

La clé du futur de la reconnaissance faciale repose, comme nous l'avons évoqué à plusieurs reprises au cours de ce livre blanc, **sur un dialogue nécessaire entre le réglementaire et la technique mais également sur un travail de démystification à mettre en œuvre au sein de la société** : le futur de la reconnaissance faciale passera par l'acceptation des individus concernés, et cette acceptation ne pourra se faire que par l'explication et l'intégration des personnes dans le projet dès le démarrage.

La crise sanitaire et économique actuelle a accéléré la prise de conscience que la technologie apporte des réponses et des solutions à des problématiques comme la sécurité et la santé. Elle permet plus de flexibilité aux entreprises qui peuvent s'appuyer sur la reconnaissance faciale pour le respect des règles de distanciation tout en conservant un très haut niveau de sécurité. Aux utilisateurs, elle réduit les contraintes et le temps dévolu aux contrôles d'authentification. Même si le temps des politiques publiques et celui de la technologie et des besoins des entreprises ne vont pas au même rythme, les besoins croissants en matière de sécurité dans les secteurs gouvernementaux, et ceux des entreprises pour l'identification et la santé des employés ou leurs affaires, devraient être des facteurs clés pour la croissance de la demande sur le marché de la reconnaissance faciale.

Remerciement

Un grand merci à

Jérémie Caron,
dirigeant du Groupe M2M Factory, spécialiste Vidéo et Sécurité

Victoria Hauser,
consultante spécialiste de la conformité et de la cybersécurité chez Synelience

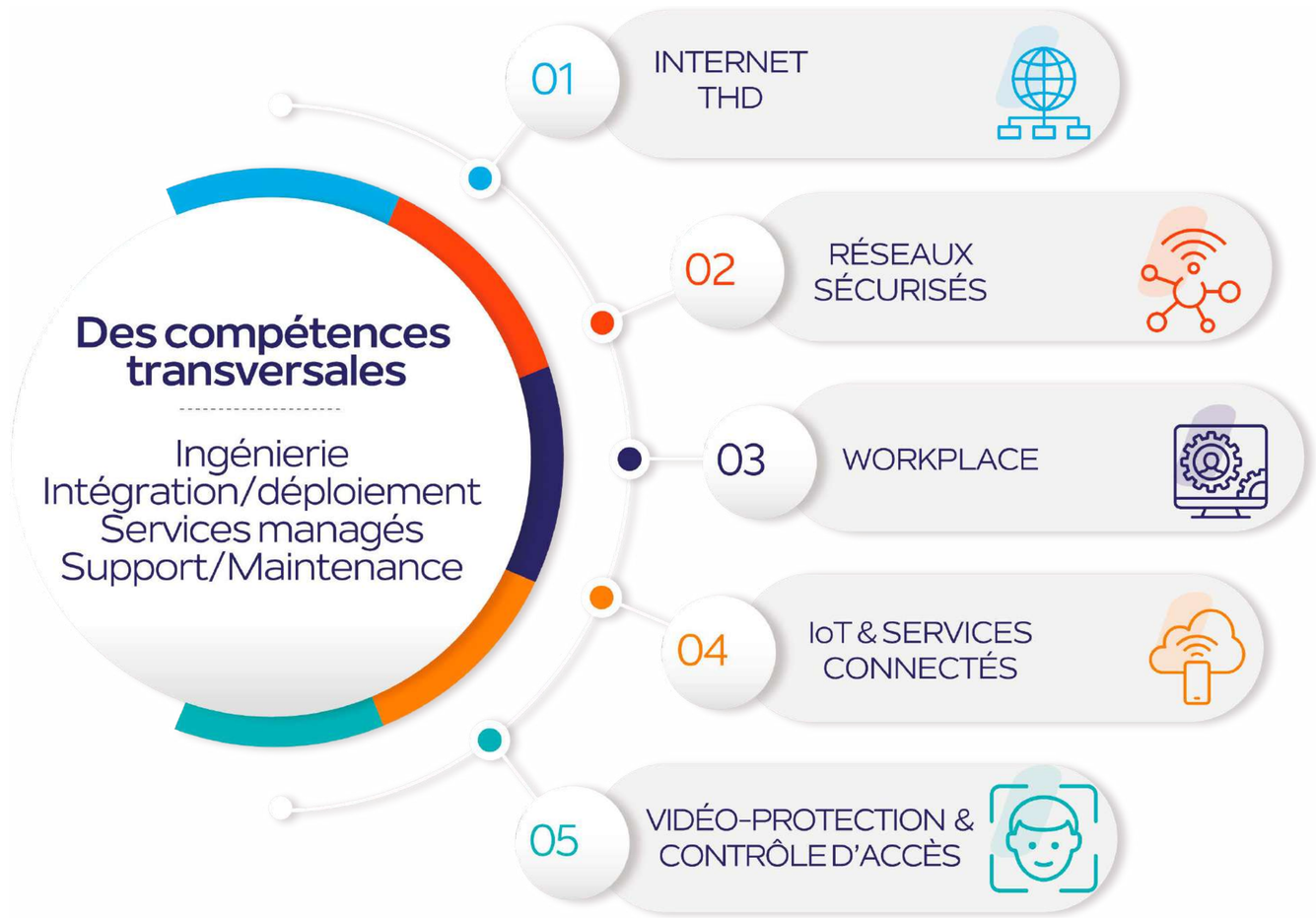
Oumaima Mounsif,
consultante risques et conformité spécialisée en intelligence économique, chez Synelience

À propos de Wixalia

Wixalia est opérateur* et intégrateur IT. Partenaire de votre connectivité, nous en avons une approche globale : du lien internet à l'IoT.

Mission :
L'ambition de Wixalia est de connecter les entreprises à l'innovation digitale et de les préparer aux nouveaux développements technologiques, notamment en matière d'intelligence artifcielle. Plus qu'un simple fournisseur d'infrastructures, nous vous accompagnons de l'expérimentation à l'indutrialisation de vos nouveaux services, avec l'agilité d'une organisation spécialisée à taille humaine.

Nos domaines d'expertise :



Wixalia.com
Tel : +(33) 01 70 83 60 70
Email : contact@wixalia.com

*déclaré à l'Arcep


Wixalia