Novembre 2019

ARTICLE

Reconnaissance faciale : les enjeux éthiques et juridiques d'une technologie qui fascine et inquiète

Technologie innovante mais décriée, la reconnaissance faciale soulève indéniablement de nombreux enjeux sociologiques et juridiques. Ses multiples possibilités d'utilisation à des fins de sécurité, en font un sujet d'intérêt majeur, tant pour les industriels et spécialistes du secteur, que pour les pouvoirs publics. L'INHESJ a chargé l'un des groupes de diagnostic stratégique de la 30e session nationale « Sécurité et Justice » de réfléchir et travailler sur les nombreux enjeux encadrant l'utilisation d'une telle technologie. Le rapport, qui dresse l'état des lieux français et international du développement de la technologie, s'intéresse aux considérations éthiques, sociologiques et juridiques inhérentes au sujet et formule des recommandations concrètes pour permettre d'apporter un début de réponse à ces problématiques contemporaines.

Introduction

La reconnaissance faciale est aujourd'hui au centre des préoccupations des autorités de contrôle européennes, comme le démontre la récente sanction de l'autorité suédoise à l'encontre d'un dispositif mis en œuvre au sein d'un lycée, dans le but de contrôler l'assiduité des élèves. Selon l'autorité de contrôle suédoise, ce dispositif n'était pas mis en œuvre conformément aux principes de limitation et de minimisation des données prévus par le règlement général sur la protection des données (RGPD) et aurait dû faire l'objet d'une analyse d'impact, eu égard à la sensibilité des données. Par ailleurs, le 15 août dernier, l'autorité de contrôle britannique (ICO) a ouvert une enquête au sujet de l'utilisation de cette technologie à King's Cross, dans le centre de Londres .

Perpétuel questionnement continuellement réévalué à mesure de l'évolution des risques et enjeux contemporains, l'équilibre entre sécurité et respect des libertés individuelles constitue l'un des marqueurs forts de l'identité culturelle française en matière de sûreté. La technologie de la reconnaissance faciale, laquelle permet de « reconnaître » de façon automatique, à partir d'une première image d'un visage fixe ou animée, ce même visage sur un autre support, s'inscrit bien dans cette problématique.

A l'heure où certains États entendent déployer des dispositifs de reconnaissance faciale de manière intensive dans l'espace public, et où cette technologie semble séduire certains de nos compatriotes pour des usages personnels, dans quelle mesure et sous quelles conditions cette technologie, encore en phase d'apprentissage, est-elle à même de connaitre un essor identique dans un contexte sécuritaire en France ?

Une technologie aboutie aux multiples cas d'usages

En faisant appel à l'intelligence artificielle et au potentiel du big data, la reconnaissance faciale offre, dans le cadre de la sphère privée, des avantages nouveaux et contribue à une fluidification, voire une sécurisation de certaines opérations. Elle constitue, pour beaucoup d'acteurs, une technologie aboutie en cours de démocratisation. Il n'en est cependant pas moins vrai que, compte tenu de son fonctionnement, fondé sur des données biométriques, par définition sensibles, et de son utilisation dans le cadre public, marquée par l'exemple d'utilisations à des fins sécuritaires particulièrement connotées (exemple de la Chine), ces dispositifs suscitent nombre d'inquiétudes et de fantasmes.

Les cas d'usages sont variés, et peuvent être utilitaires, commerciaux, ou encore sécuritaires : facilités d'accès à des services bancaires, accueil personnalisé, mais aussi recensement ou fiabilisation de vote électronique en luttant contre la fraude à l'identité, renforcement de la protection de sites sensibles et stratégiques, etc. Les exemples d'utilisation à l'étranger sont multiples, et en large progression, le cas le plus avancé et médiatisé étant celui de la Chine, où la reconnaissance faciale est notamment devenu un procédé courant pour appréhender des personnes recherchées.

En France, en revanche, les exemples sont plus limités, et restent cantonnés à des contextes très encadrés et le plus souvent expérimentaux. Aussi, la crainte de l'instauration d'une société de surveillance se renforce-t-elle de l'opacité de la mise en œuvre de technologies dont la majorité de la population craint qu'elles puissent être opérationnelles à son insu.

Des défis techniques pour les industriels français

Le marché de la reconnaissance faciale est en très forte croissance, et les industriels français bénéficient d'une réputation d'excellence et d'une longue expérience de la biométrie, ce qui les place idéalement sur ces marchés. Cependant, ils font face à une difficulté de taille puisque la performance de ces technologies leur impose désormais de disposer de très importantes bases de données.

D'un point de vue technique, les capacités d'analyse et la fiabilité des résultats obtenus par les industriels sont étroitement dépendantes de la qualité des données traitées et des algorithmes utilisés, semble-t-il encore très perfectibles, puisque la reconnaissance faciale demeure à ce jour un outil d'aide à la décision nécessitant d'être confirmée par une validation humaine. Le développement de l'auto-apprentissage des algorithmes repose en effet sur la faculté pour les laboratoires de recherche d'utiliser des bibliothèques de visages.

Sur le plan juridique, la réglementation relative à la protection des données à caractère personnel, applicable en l'espèce, encadre strictement le traitement de données biométriques, puisqu'il est par principe interdit ; il ne peut être opéré que si la personne concernée a donné son consentement explicite ou si ce traitement est nécessaire pour des motifs d'intérêt public importants, et est alors autorisé par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés (CNIL). En conséquence, les industriels français se

heurtent à l'absence de cadre légal leur permettant, sauf exception, de tester leurs solutions en conditions réelles sur le territoire, ce qui n'est pas le cas dans d'autres pays.
Comme en fait état le rapport INHESJ sur le sujet, il résulte de ces éléments que le maintien d'un rôle et d'une place significatifs par les acteurs industriels français en cette matière nécessite au préalable qu'ils soient en mesure de parfaire les performances des algorithmes.
De plus, les risques relatifs à la cyber-sécurité ne peuvent être exclus, en raison des possibilités de contourner cette technologie par le biais de leurres (faux visages), ou de dérober des données, alors non modifiables bien que compromises ! Le vol de données est sans nul doute l'une des principales menaces qui visent les systèmes biométriques. A cet égard, de nombreux exemples de compromission sont régulièrement relayés sur Internet. Face aux menaces et aux vulnérabilités, il convient indéniablement d'apporter une attention particulière à la mise en place de mesures de cyber-sécurité adaptées aux dispositifs de reconnaissance faciale.

Une acceptation sociétale inégale

L'acceptation par la population d'un éventuel déploiement de la reconnaissance faciale sur le domaine public constitue un véritable défi, quand bien même son efficacité pour prévenir la commission d'infractions aurait été prouvée.
Traditionnellement, la culture occidentale reste réservée à l'égard de toute intrusion et surveillance de ce qui relève de la vie privée ; et ce en dépit de l'ambivalence que nous démontrons à l'égard de ces nouvelles technologies, ainsi que de notre propre intimité. Pour autant, il semble que de manière générale, la population, manifestement sensible au contexte sécuritaire, soit moins réticente aux lois restrictives de liberté, et que la « risquophobie » plaide désormais pour une société de plus en plus protectrice. Ce renoncement à ce que d'aucuns peuvent considérer comme un pan de liberté ne saurait toutefois avoir lieu sans que soient a minima apportées des garanties afin de trouver le juste équilibre entre l'exigence de contrôle et le respect de la vie privée.
Le développement de la reconnaissance faciale ne saurait se faire sans avoir acquis la confiance de la population. Aussi, tel qu'en font état les résultats des travaux du groupe de travail INHESJ, il semble indispensable de garantir l'information, la communication et le dialogue avec les personnes concernées autour de la mise en œuvre de tels dispositifs, et plus particulièrement s'agissant des espaces publics soumis à un dispositif de reconnaissance faciale.

Un encadrement juridique encore insuffisant

L'étude du cadre juridique existant révèle l'absence de dispositions légales et règlementaires spécifiques dédiées aux expérimentations de technologies nouvelles. De plus, les données biométriques traitées lors de la mise en œuvre des dispositifs de reconnaissance faciale sont strictement encadrées par les dispositions relatives à la protection des données. Ces traitements, par principe prohibés, ne connaissent pas non plus de dérogation particulière en matière d'expérimentation. L'absence de cadre juridique spécifique représente ainsi un frein à la mise en œuvre des expérimentations. Il en ressort donc que la possibilité de tester l'efficacité des dispositifs de reconnaissance faciale dans des contextes factuels réalistes et notamment parmi les foules, reste considérablement limitée et contrainte.
Les travaux du groupe de diagnostic stratégique relèvent qu'il serait donc utile d'élaborer un cadre juridique dédié afin de faciliter la faisabilité juridique des expérimentations sur les dispositifs de reconnaissance faciale. En application de l'article 9 du RGPD, les Etats membres

de l'Union européenne sont en mesure de prévoir des conditions supplémentaires dans le cadre desquelles les traitements de données biométriques pourraient être réalisés. A ce titre, il pourrait être pertinent d'encadrer, par exemple par décret, les cas d'usage précis où des expérimentations pourraient être menées, tels que des grands évènements, des complexes sportifs ou culturels, des sites privés ouverts au public à enjeux sécuritaires importants, les conditions matérielles de leur mise en œuvre, etc.

Il s'agirait également d'envisager qu'un texte législatif, soumis à l'étape préalable du débat démocratique, vienne encadrer les cas et situations dans lesquels les autorités compétentes seraient autorisées à utiliser des technologies de reconnaissance faciale. Ce texte permettrait notamment de déterminer les motifs pour lesquels de tels traitements pourraient être mis en œuvre, ainsi que les modalités de déclenchement des dispositifs par une autorité (préfet, magistrat). Il semble en outre que la question de l'unification et de la centralisation des fichiers utilisés à des fins de comparaison devrait également être traitée.

Propos conclusifs

Compte tenu des enjeux en termes de souveraineté, il est important que la France puisse occuper une place de choix dans ce challenge technologique mondial que représente le développement de la reconnaissance faciale, afin de bénéficier des emplois et ressources associés à ce marché porteur, de disposer d'une technologie totalement maitrisée pour les déploiements à forte connotation sécuritaire ou souveraine, et de rester dans la compétition sécuritaire et technologique afférente à l'organisation de grands événements planétaires (Coupe du monde de rugby 2023, Jeux Olympiques 2024, etc.).

Au centre de cette démarche, la préservation des intérêts fondamentaux des citoyens, et notamment de leurs libertés individuelles et de leur vie privée, doit rester le fil conducteur.