Technologies biométriques : un risque pour chacun d'entre nous

Description

Outre la question importante des atteintes à la vie privée, le recours à la biométrie pour l'authentification, l'identification et l'évaluation des personnes comporte *« un potentiel inégalé d'amplification et d'automatisation des discriminations »*, avertit la Défenseure des droits dans un rapport consacré aux technologies biométriques publié en juillet 2021.

Telle que définie par la Commission nationale de l'informatique et des libertés (Cnil), la biométrie est *« l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales, etc.) »*. Empreintes digitales, veines de la paume de la main, échantillon de voix, traits du visage, iris de l'œil, ainsi que certains comportements comme le rythme de la frappe sur un clavier, ces caractéristiques qualifiées de « données sensibles » par le RGPD peuvent servir à identifier ou reconnaître une personne, notamment à son insu.

À mesure qu'elles se perfectionnent, les technologies biométriques sont déployées dans l'espace public comme dans l'entreprise, dans le secteur privé comme dans le secteur public. En se généralisant, la collecte de « données sensibles », avec ou sans le consentement des personnes concernées, constitue d'immenses bases de données – les données étant les caractéristiques physiques et uniques des personnes –, qui alimentent le calcul des algorithmes d'apprentissage, lesquels permettent aux systèmes biométriques de fonctionner. Très intrusives, les technologies biométriques représentent *« des risques considérables d'atteinte aux droits fondamentaux »*, selon la Défenseure des droits, Claire Hédon.

Il existe trois sortes de techniques biométriques qui se distinguent selon leur finalité. Les systèmes d'authentification servent à vérifier l'identité déclarée d'une personne à partir d'un support sécurisé, tel qu'un passeport, un badge ou un téléphone, sur lequel sont stockées les données personnelles la caractérisant ; ils n'ont donc pas recours à une base de données. Les systèmes d'identification à distance, quant à eux, sont destinés à retrouver une personne parmi une foule d'individus ; ils sont alors capables, en temps réel, de croiser une image prise par une caméra de vidéosurveillance avec des millions d'autres enregistrées dans une base de données. Claire Hédon souligne à ce propos que *« l'identification implique la collecte de données sensibles parfois à une échelle extrêmement importante, sans savoir au préalable si la personne recherchée figurera parmi les personnes examinées »*. L'usage des systèmes biométriques d'authentification et d'identification répond souvent à des objectifs de sécurité publique comme la surveillance d'un lieu public ou le déroulement d'une enquête judiciaire.

La troisième catégorie de techniques biométriques, la plus récente, appelée système d'évaluation, fonctionne soit pour déduire la personnalité d'un individu à partir de la « reconnaissance d'émotions », soit pour inscrire un individu dans une catégorie spécifique selon l'âge, le sexe, la couleur des yeux, l'origine ethnique, l'orientation sexuelle ou politique. Ce type d'évaluation biométrique des personnes est déjà pratiqué dans le monde de l'entreprise, où serait par exemple analysée et mesurée automatiquement la nervosité d'un candidat à l'embauche. D'autres mesures biométriques seraient réalisables pour évaluer la concentration d'un étudiant, la fatigue d'un automobiliste ou la propension d'une personne à commettre une infraction. *« Les fondements scientifiques de ces technologies font l'objet de vives critiques de la part de la communauté scientifique, en particulier s'agissant des technologies de détection d'émotions ou de reconnaissance de l'affect »*, alerte la Défenseure des droits. Sortis de leur contexte, des extraits de voix ou des expressions du visage ne sont pas des éléments fiables et précis pour définir une émotion, et encore moins pour évaluer des qualités professionnelles.

Il faut aussi distinguer les technologies actives, pour lesquelles la personne fournit elle-même des informations, et les technologies passives qui captent des données souvent sans prévenir, car les risques ne sont pas les mêmes quand les informations personnelles sont stockées sur un support individuel ou lorsqu'elles sont centralisées et traitées dans une base de données. La Défenseure des droits voit un potentiel de risques importants avec le déploiement tous azimuts de technologies passives, telle la vidéosurveillance, à l'aide de caméras-piétons ou de drones, qui se répand dans la rue, les transports, les magasins, les halls d'immeuble. Un phénomène qui *« s'accompagne en droit d'un assouplissement des conditions de transmission aux services de police des images enregistrées par de multiples acteurs comme de l'interopérabilité et de l'interconnexion de nombreux fichiers »*, explique-t-elle. Au Royaume-Uni, l'opposition de la société civile a mené à l'abandon d'un dispositif de contrôle combinant pass sanitaire et reconnaissance faciale.

Outre les atteintes à la vie privée, la Défenseure des droits souligne particulièrement le *« potentiel inégalé d'amplification et d'automatisation des discriminations »* des technologies biométriques. La généralisation de l'usage de ces systèmes qui exploitent des caractéristiques humaines – caractéristiques souvent elles-mêmes à l'origine de discriminations telles que l'origine, le sexe, le genre, l'apparence – risque précisément de perpétuer et d'amplifier les discriminations dont sont déjà victimes certains groupes sociaux, comme l'ont démontré de nombreuses études portant sur le profil des personnes victimes d'une erreur. Les algorithmes d'apprentissage sont potentiellement discriminatoires par l'emploi de bases de données qui ne reflètent pas la diversité de la population. Régulièrement présenté comme très faible, notamment pour la reconnaissance faciale, leur taux d'erreur – soit le pourcentage de faux-positifs ou de faux-négatifs – implique en réalité qu'une technologie biométrique installée dans un espace public est susceptible d'affecter une multitude de personnes. En 2020, la Cour d'appel de Londres a rendu une décision inédite en la matière, concluant que les services de police n'avaient pas été assez vigilants quant aux risques de discrimination liés aux biais d'un logiciel de reconnaissance faciale auquel ils avaient eu recours.

Des risques de discrimination peuvent également provenir de l'utilisation même des outils de mesure

biométrique. Ainsi, les systèmes d'évaluation lors d'une procédure de recrutement sont d'emblée discriminants au regard des candidats en situation de handicap qui présenteront une manière de s'exprimer ou de se tenir différente de la grande majorité.

Enfin, l'une des conséquences inquiétantes du déploiement des technologies biométriques dans les lieux publics est *« l'effet dissuasif »* qu'elles peuvent susciter sur *« l'exercice des droits fondamentaux comme la liberté d'expression, d'aller et venir, d'assemblée, d'association, et, plus largement, l'accès aux droits »*. *« En l'absence de friction »*, c'est-à-dire en fonctionnant sans qu'elles le sachent et sans qu'elles puissent contrôler quoi que ce soit, les techniques biométriques ont tendance à modifier le comportement des personnes concernées. *« L'un des aspects nécessaires dans l'exercice de ces libertés repose effectivement sur l'anonymat de groupe, en l'absence duquel les individus peuvent être amenés à altérer leur comportement et à ne pas exprimer leurs pensées de la même manière »*, explique la Défenseure des droits. Avant d'être censurée par le Conseil constitutionnel, la loi pour une sécurité globale préservant les libertés, promulguée en mai 2021, en instaurant la possibilité pour les services de police d'utiliser des drones équipés de caméras était susceptible d'avoir un *« effet dissuasif »* à participer à des manifestations de rue (voir *La rem* n°57-58, p.5).

Concluant son rapport par une série de recommandations, la Défenseure des droits insiste notamment sur la nécessité de veiller systématiquement à la pertinence d'une technologie biométrique avant son déploiement et, dans le prolongement de cette précaution, d'interdire les technologies n'apportant aucune garantie scientifique, tel le système biométrique d'évaluation des émotions. Est également recommandé un contrôle régulier des algorithmes au cours de leur fonctionnement afin de prévenir, comme pour les médicaments, de *« leurs effets indésirables »*.

À l'approche des jeux Olympiques de Paris de 2024, les débats parlementaires sur la question de la sécurité donnent toute son importance à l'avertissement formulé par la Défenseure des droits.

Source :

- Technologies biométriques : l'impératif respect des droits fondamentaux, Défenseur des droits, République française, defenseurdesdroits.fr, juillet 2021.

Categorie

1. Usages

date créée
22 décembre 2021
Auteur

francoise