Société

Technologies biométriques : dangers et recommandations
Prévenir les biais discriminatoires et les atteintes aux droits

Dans un rapport du 8 juillet 2021, le Défenseur des droits appelle à renforcer l'encadrement des technologies biométriques et de leurs usages multiples [(1)].

RÉPUBLIQUE FRANÇAISE
LE DÉFENSEUR DES DROITS

Allant du simple déverrouillage d'un téléphone portable à *« la supposée analyse des émotions d'un candidat à l'embauche »*, le déploiement des technologies biométriques s'est considérablement accéléré, ces dernières années, en France comme dans toute l'Europe. Ces technologies sont mobilisées dans des domaines très variés comme *« le recrutement et la gestion des ressources humaines, l'accès aux biens et services, la sécurité, ou encore l'éducation ».*

La multiplication de ces usages est liée aux dernières avancées des algorithmes d'apprentissage dont *« les puissances de calcul permettent désormais une exploitation massive de grands ensembles de données, promettant optimisation et gains de productivité ».* Si ces technologies présentent des avantages, *« elles sont particulièrement intrusives et comportent un certain nombre de risques pour la protection des données et de la vie privée »,* comme la Commission nationale de l'informatique et des libertés (Cnil) a pu le relever à plusieurs reprises. Ces risques doivent également être considérés *« sous l'angle de leur impact sur les droits fondamentaux ».*

Actuellement, des propositions pour renforcer l'encadrement des technologies biométriques sont à l'étude en France et à l'échelle européenne : elles visent à *« s'assurer du respect des droits des individus au-delà de la seule et nécessaire protection des données à caractère personnel »,* mais également à prévenir les biais discriminatoires des algorithmes et de *« l'usage exponentiel de ceux-ci dans toutes les sphères de la vie sociale ».*

Réaliser une transaction avec la paume de sa main, identifier automatiquement un suspect dans une foule, proposer de la publicité ciblée à une personne en fonction de son apparence physique… Autant d'actions rendues possibles par *« des techniques informatiques de reconnaissance et/ou d'évaluation physique, biologique ou comportementale des individus »,* qui permettent de collecter et de traiter des *« caractéristiques biométriques ».* Ces données sont stockées sous format numérique et enregistrent les caractéristiques physiques uniques des personnes pour les distinguer.

En France, les premières utilisations de technologies biométriques remontent au début du XX^{e}. Ce sont les services de police qui ont commencé à collecter les empreintes digitales des personnes soupçonnées d'avoir commis un crime. Pendant longtemps, ces technologies étaient réservées à *« quelques cas d'usage bien définis tels que l'établissement d'un passeport respectant certaines normes de sécurité, ou l'analyse d'un échantillon ADN afin d'établir la paternité d'une personne ».*

Les systèmes d'authentification, d'identification et d'évaluation

Avec les avancées scientifiques dans le champ des algorithmes d'apprentissage, ces usages se sont diffusés à travers les outils numériques et connectés : *« Reconnaissance faciale, vocale, évaluation des émotions, les utilisations de nos données biométriques sont désormais légion ».* À ce jour, on distingue trois types de systèmes biométriques : les systèmes d'authentification, les systèmes d'identification et les systèmes d'évaluation.

(1) – « Technologies biométriques : l'impératif respect des droits fondamentaux » (29 pages).

CÉAS de la Mayenne – Septembre 2021

L'authentification consiste à vérifier si une personne est bien celle qu'elle affirme être : c'est le cas pour l'utilisation des passeports biométriques des voyageurs mais aussi pour sécuriser l'accès physique d'un bâtiment, ou encore effectuer un paiement.

Quant à l'identification, elle vise à retrouver une personne parmi un grand nombre d'individus, dans un lieu, sur une image, ou dans une base de données : *« Les techniques d'identification les plus récentes ont pour particularité de pouvoir potentiellement s'appliquer à un nombre illimité d'individus sans qu'ils en aient même conscience ».* Cela peut concerner la surveillance d'espaces publics lors d'événements, les enquêtes judiciaires ou encore la lutte contre l'immigration illégale.

Aux systèmes d'authentification et d'identification s'ajoutent les systèmes d'évaluation qui ont pour objectif de *« déduire les traits de personnalité d'un individu et catégoriser les personnes en fonction de leurs caractéristiques biométriques ».*

Ces systèmes – alliant authentification et identification – peuvent permettre à certaines entreprises d'analyser et de mesurer automatiquement *« la nervosité d'un candidat ou d'une candidate dans le cadre d'une procédure de recrutement »*. Il peut aussi s'agir d'évaluer la concentration d'un étudiant, la fatigue d'un automobiliste, la *« propension d'une personne à commettre une infraction dans un environnement donné »,* ou encore les réactions d'un consommateur à la présentation de biens ou de services dans le but de lui proposer de la publicité ciblée.

Le Défenseur des droits souligne les *« vives critiques »* formulées par la communauté scientifique à l'égard des technologies biométriques. En particulier, celles qui visent la détection d'émotions ou la reconnaissance de l'affect : *« De nombreuses personnalités appellent à en encadrer strictement les usages ».* La littérature scientifique démontre que ces technologies sont *« biaisées et commettent de nombreuses erreurs ».* En effet, les émotions humaines dépendent d'un contexte allant bien au-delà du visage et du corps. Aussi est-il impératif d'interroger la fiabilité et la précision de ces technologies.

Ces systèmes sont régulièrement présentés comme *« efficients »* à des services de ressources humaines alors qu'ils sont, dans les faits, *« très pauvrement corrélés à l'efficacité au travail ».* En outre, les risques de discrimination et d'atteintes aux libertés liés à leur utilisation dans le champ de l'emploi comme dans d'autres domaines doivent être *« mieux connus et soulignés plus clairement ».* Si ces systèmes présentent des avantages notamment dans la lutte contre la criminalité, il n'en demeure pas moins qu'ils reposent sur l'exploitation de données particulièrement sensibles, laquelle *« pourrait porter atteinte au droit au respect de la vie privée comme au droit de la protection des données ».*

Évaluer les risques d'atteintes aux droits fondamentaux

Les données biométriques sont avant tout *« probabilistes »* et, en aucun cas, absolues. Au-delà des marges d'erreurs, les données recueillies par les technologies biométriques ciblent le plus souvent les caractéristiques personnelles des individus (âge, origine, identité de genre, état de santé, handicap, apparence physique…). En ce sens, la généralisation de leur usage est susceptible de *« perpétuer voire d'amplifier, pour certains groupes sociaux, les discriminations systémiques opérant au sein de la société ».*

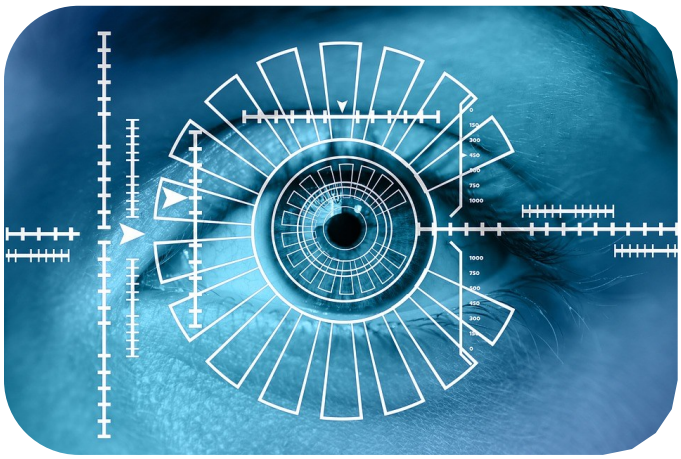
Les conséquences du caractère probabiliste et potentiellement discriminatoire de ces données peuvent aller *« du refus d'accès physique à un lieu ou à un événement à une arrestation erronée par les forces de l'ordre ».* En outre, de nombreuses études ont démontré que les profils des personnes victimes de ces erreurs renvoient majoritairement à des *« personnes issues de groupes discriminés et/ou vulnérables (femmes, enfants mineurs, personnes transsexuelles, personnes à la peau foncée, entre autres) ».*

Le Défenseur des droits adresse une liste de recommandations afin d'inviter les pouvoirs publics et les utilisateurs du secteur privé à *« interroger davantage les conséquences pour les droits et libertés du déploiement des technologies biométriques ».* Ces recommandations s'articulent autour de trois axes : écarter les méthodologies d'évaluation non pertinentes ; mettre en place des garanties fortes et effectives pour s'assurer du respect des droits des individus ; repenser les contrôles existants.

Le Défenseur des droits mentionne un point de vigilance concernant *« le déploiement de technologies fondées sur des méthodologies non éprouvées scientifiquement »* et en appelle à la responsabilité des acteurs. Il s'agit notamment de tenir compte des risques significatifs de détournement et d'encadrer les usages à des fins policières : *« En tout état de cause, le recours à l'identification biométrique ne saurait concerner tout type*

d'infraction ». Les systèmes de surveillance tels les caméras piétons, la vidéosurveillance, l'usage des drones pour capter des images, doivent être rigoureusement encadrés.

Par ailleurs, *« le droit au recours des personnes victimes de discriminations doit être assuré et facilité par l'entité publique comme privée responsable du traitement ».* Les garanties de droit d'accès aux usagers doivent être préservées au même titre que *« la réalisation des démarches administratives dématérialisées doit demeurer une possibilité ouverte à l'usager et non devenir une obligation ».*



Les analyses d'impact relatives à la protection des données imposées par l'article 35 du Règlement général sur la protection des données (RGPD) font référence au *« risque élevé que peut engendrer un traitement pour les droits et libertés des personnes physiques ».* Pour cette raison, le Défenseur des droits recommande de réviser le seuil d'évaluation des marchés publics informatiques et *« d'intégrer à leur contrôle, au-delà des seuls aspects budgétaires, une appréciation des risques de discrimination, et plus généralement d'atteintes aux libertés et droits fondamentaux ».*

Le Défenseur des droits invite le législateur à *« s'inspirer largement de la proposition de réglementation de l'intelligence artificielle de la Commission européenne ».* Pour les fournisseurs de technologies biométriques d'identification à distance, la Commission européenne prévoit notamment l'obligation de respecter certaines exigences strictes en termes de transparence et d'évaluation des risques avant toute mise en œuvre et toute commercialisation de ces systèmes.

Enfin, le Défenseur des droits rappelle sa recommandation *« en faveur d'un contrôle régulier des effets des algorithmes »* : il s'avère impératif de ne pas automatiser ce type d'intelligence artificielle – comme il est d'usage actuellement pour évaluer les effets indésirables des médicaments – sans un encadrement bien défini.