RAPPORT

Technologies biométriques : l'impératif respect des droits fondamentaux

Face au droit, nous sommes tous égaux

Défenseurdesdroits
RÉPUBLIQUE FRANÇAISE

RAPPORT

Technologies biométriques : l'impératif respect des droits fondamentaux

PROPOS LIMINAIRES

Au cours des dernières années, le déploiement de dispositifs biométriques s'est fortement accéléré en France comme dans toute l'Europe. Secteurs public et privé confondus, ces technologies sont désormais mobilisées dans des domaines aussi variés que le recrutement et la gestion de ressources humaines, l'accès aux biens et services, la sécurité, ou encore l'éducation. Cette multiplication des usages est étroitement liée aux dernières avancées des algorithmes d'apprentissage sur lesquels ces technologies s'appuient largement et dont les puissances de calcul permettent désormais une exploitation massive de grands ensembles de données, promettant optimisation et gains de productivité.

Allant du simple déverrouillage d'un téléphone portable à la supposée analyse des émotions d'un candidat à l'embauche, ces technologies ont toutes pour point commun de traiter des données biométriques telles que les traits du visage, la voix ou les caractéristiques comportementales des individus, dans le but d'authentifier, d'identifier ou d'évaluer ces derniers. Désormais, il est possible de réaliser une transaction avec la paume de sa main comme d'identifier automatiquement un suspect dans une foule, ou encore de proposer de la publicité ciblée à un individu en fonction de son apparence physique.

Quand bien même ces technologies peuvent présenter un certain nombre d'avantages, elles sont particulièrement intrusives et comportent un certain nombre de risques pour la protection des données et de la vie privée, ce que la Commission Nationale de l'Informatique et des Libertés (CNIL) a pu relever à plusieurs reprises[1].

Au-delà de ces aspects, les risques doivent également être considérés sous l'angle de leur impact sur les droits fondamentaux dont le Défenseur des droits assure la protection dans l'ensemble de ses champs de compétence : lutte contre les discriminations, respect de la déontologie par les personnes exerçant des activités de sécurité, protection des droits de l'enfant, accès aux droits et aux services publics.

En mai 2020, le Défenseur des droits appelait, conjointement avec la CNIL, à une mobilisation collective pour prévenir les biais discriminatoires des algorithmes, dénoncer les risques considérables de discrimination que peut faire peser sur chacun et chacune d'entre nous l'usage exponentiel de ceux-ci dans toutes les sphères de la vie sociale et renforcer le cadre juridique applicable[2]. Les conséquences de ces biais étant particulièrement prégnantes en matière de biométrie, il est apparu essentiel de poursuivre cette réflexion afin d'anticiper les futures saisines de l'institution et d'appeler les pouvoirs publics comme les utilisateurs du secteur privé à interroger davantage les conséquences pour les droits et libertés du déploiement des technologies biométriques.

À l'heure où des propositions pour renforcer l'encadrement de ces technologies sont étudiées tant à l'échelle européenne qu'en France, le Défenseur des droits souhaite adresser une liste de recommandations qui lui paraissent indispensables pour s'assurer du respect des droits des individus au-delà de la seule et nécessaire protection des données à caractère personnel.

TECHNOLOGIES BIOMÉTRIQUES : UN TERME GÉNÉRIQUE ENGLOBANT UNE PLURALITÉ D'USAGES

Techniques informatiques de reconnaissance et/ou d'évaluation physique, biologique ou comportementale des individus[3], les technologies biométriques partent toutes d'un même procédé : les caractéristiques biométriques collectées sont traitées selon des procédures standardisées et le résultat de ce processus est stocké dans des enregistrements de données appelés signatures, modèles ou gabarits. Ceux-ci concentrent sous format numérique les caractéristiques physiques uniques des personnes permettant de les différencier[4].

Les premières utilisations de technologies biométriques remontent en France au début du XXe siècle. En 1902, les services de police ont commencé à collecter les empreintes digitales des personnes soupçonnées d'avoir commis un crime[5], et, pendant longtemps, ces technologies se sont cantonnées 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.

Sous l'effet des avancées scientifiques dans le champ des algorithmes d'apprentissage, ces usages se sont aujourd'hui multipliés. **Reconnaissance faciale, vocale, évaluation des émotions, les utilisations de nos données biométriques sont désormais légion**.

On distingue aujourd'hui trois types de systèmes biométriques : les systèmes d'authentification, les systèmes d'identification et les systèmes d'évaluation.

AUTHENTIFICATION : DÉTERMINER SI UNE PERSONNE EST BIEN CELLE QU'ELLE AFFIRME ÊTRE

L'authentification consiste à vérifier l'identité revendiquée par quelqu'un en comparant les données biométriques d'une personne à un instant T à celles de l'identité attestée qu'elle revendique[6].

La fonction de déverrouillage par reconnaissance faciale d'un téléphone portable où la photographie de l'utilisateur est comparée à celle qu'il a préalablement enregistrée sur l'appareil lors de son paramétrage[7], ou encore le dispositif européen de contrôle du passage aux frontières PARAFE[8] où les gabarits stockés dans les passeports biométriques des voyageurs sont comparés à ceux que réalisent des portiques dédiés[9] relèvent, par exemple, d'un objectif d'authentification.

En pratique, les technologies biométriques d'authentification permettent de comparer les gabarits d'une personne stockés sur un support sécurisé (un badge, un passeport, un téléphone) à la partie du corps ou à une caractéristique du corps de cette prétendue même personne (traits du visage, bout des doigts, iris de l'œil, forme de la main, échantillon de voix, etc.) afin de déterminer s'il existe effectivement une correspondance entre les deux.

Ces systèmes peuvent être utilisés pour sécuriser l'accès physique à un bâtiment, effectuer un paiement, passer une frontière, etc. En termes de droit au respect de la vie privée, leur avantage est qu'ils restent généralement sous le contrôle exclusif des personnes et leur bon fonctionnement n'exige pas d'avoir recours à une base de données centralisée. Pour reprendre les exemples précités, lors du paramétrage de la fonction de déverrouillage du téléphone ou de la création du passeport biométrique, les gabarits contenant les caractéristiques importantes du visage (distance entre les yeux, forme du menton) sont chiffrés puis stockés localement sur le téléphone ou sur la puce implantée dans le passeport. De fait, les personnes restent généralement libres de les utiliser ou non.

IDENTIFICATION : RETROUVER UNE PERSONNE PARMI UNE MULTITUDE D'INDIVIDUS

L'identification vise à retrouver une personne au sein d'un groupe d'individus, dans un lieu, sur une image[10], ou dans une base de données à partir notamment des traits du visage (reconnaissance faciale)[11], de la voix (reconnaissance du locuteur)[12], du comportement (reconnaissance de la démarche)[13] ou de tout autre type de donnée biométrique.

À l'instar de certaines technologies de reconnaissance faciale, un système d'identification permet de réaliser l'opération suivante : le gabarit tiré des traits du visage d'une personne est comparé au moyen d'un algorithme à une pluralité d'autres gabarits stockés sur une base de données afin de déterminer l'identité de la personne. Cette même démarche s'applique aux gabarits extraits d'autres parties du corps en fonction du type de technologie biométrique d'identification considéré. En d'autres termes, les technologies d'identification croisent les données biométriques de personnes filmées, photographiées, ou enregistrées avec une liste de personnes recherchées.

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. La Commission européenne s'est penchée sur ces systèmes d'identification biométriques à distance[14] : ils peuvent opérer « en temps réel » à partir de données collectées et analysées instantanément, comme *a posteriori*, à partir d'images tirées de caméras de vidéosurveillance ou d'autres données préexistantes. Quels que soient la technologie, les procédés ou types de données biométriques employés, **l'identification implique la collecte de données sensibles[15] parfois à une échelle extrêmement importante, sans savoir au préalable si la personne recherchée figurera parmi les personnes examinées[16]**.

À ce jour, des usages de technologies biométriques d'identification à distance ont été répertoriés en Europe essentiellement dans le domaine de la sécurité, par exemple dans le cadre de la surveillance d'espaces publics pendant des événements[17], à l'occasion d'enquêtes judiciaires[18], à des fins policières[19] ou encore de lutte contre l'immigrantion illégale[20].

ÉVALUATION : DÉDUIRE LES TRAITS DE PERSONNALITÉ D'UN INDIVIDU ET CATÉGORISER LES PERSONNES EN FONCTION DE LEURS CARACTÉRISTIQUES BIOMÉTRIQUES

Aux systèmes d'authentification et d'identification s'ajoute une troisième catégorie, plus récente, que nous appellerons ici systèmes d'évaluation.

Partant des données biométriques d'un ou de plusieurs individus, les technologies d'évaluation visent à effectuer deux actions majeures :

- Identifier ou déduire des émotions, des traits de personnalité ou des intentions (on parle alors de systèmes de « reconnaissance d'émotions »)[21];

- Inscrire la ou les personnes visées dans des catégories spécifiques, par exemple de sexe, d'âge, de couleur de cheveux, de couleur des yeux, d'origine ethnique ou d'orientation sexuelle ou politique en vue de prendre des mesures spécifiques (on parle alors de systèmes de « catégorisation »[22]).

Aujourd'hui, certaines entreprises affirment, par exemple, pouvoir analyser et mesurer automatiquement à partir de données biométriques la nervosité d'un candidat ou d'une candidate dans le cadre d'une procédure de recrutement[23]. D'autres systèmes promettent de mesurer la concentration d'un étudiant[24], la fatigue d'un automobiliste[25], la dangerosité ou la propension d'une personne à commettre une infraction dans un environnement donné[26], ou encore les réactions d'un consommateur ou d'une consommatrice à la présentation de biens ou de services afin notamment de lui proposer de la publicité ciblée[27]. Enfin, certains se proposent de profiler les individus en fonction de leurs caractéristiques physiques apparentes afin de restreindre l'accès aux biens et services qu'ils proposent à un public spécifique[28].

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**. De nombreuses personnalités appellent à en encadrer strictement les usages[29].

La littérature scientifique existante démontre en effet que ces technologies sont très biaisées et commettent de nombreuses erreurs[30]. Pour les chercheurs, détecter les émotions d'une personne avec précision et fiabilité dépendrait d'un contexte allant au-delà du visage et du corps[31].

Des échantillons de voix ou onomatopées[32] comme des mouvements du visage[33] ne suffiraient pas à caractériser des émotions humaines, et encore moins à évaluer avec rigueur les futures performances d'un candidat à l'embauche… Or ces systèmes sont régulièrement présentés à des services de ressources humaines comme particulièrement efficients alors qu'ils sont en réalité très pauvrement corrélés à l'efficacité au travail, ainsi qu'en témoigne le cas des tests de personnalité[34]. Les risques de discrimination ou d'atteintes aux libertés liés à leur utilisation dans le champ de l'emploi comme dans d'autres champs doivent être mieux connus et soulignés plus clairement.

A priori, les traitements de données biométriques aux fins d'évaluation ne relèvent pas de l'article 9 du Règlement général sur la protection des données (ci-après, RGPD) et ne constituent donc pas des traitements de « catégories particulières » de données. Si une telle interprétation n'est pas encore stabilisée, le Défenseur des droits recommande que ces méthodes d'évaluation fassent l'objet de mesures de protection spécifiques car elles mobilisent le même type de données que les traitements aux fins d'identification et leurs usages sont tout aussi risqués. Par ailleurs, des systèmes biométriques d'évaluation peuvent être combinés avec des systèmes d'identification.

DES RISQUES CONSIDÉRABLES D'ATTEINTES AUX DROITS FONDAMENTAUX

Si certains systèmes biométriques présentent des avantages indéniables dans la lutte contre la criminalité, pour garantir la sécurité publique ou dans d'autres circonstances où une identification sûre et fiable des personnes est nécessaire, ces technologies ne sauraient en aucun cas être considérées comme purement inoffensives.

Le fonctionnement de ces systèmes repose sur l'exploitation de données particulièrement sensibles qui pourrait porter atteinte au droit au respect de la vie privée comme au droit de la protection des données.

Qu'il s'agisse d'authentifier, d'identifier ou d'évaluer les individus, ces systèmes sont par nature probabilistes (ils ne peuvent estimer qu'un « pourcentage » de correspondance ou de risque) et la fiabilité de leurs résultats ne saurait donc être considérée comme absolue. Ainsi, non seulement les algorithmes sur lesquels ils reposent peuvent comporter, dès leur conception, des biais discriminatoires mais ils peuvent générer des erreurs d'allocation ou de sélection, aux conséquences particulièrement importantes pour les individus concernés.

Enfin, certains usages, en particulier en matière d'identification et d'évaluation, peuvent engendrer un effet dissuasif dans l'exercice de certains droits fondamentaux (liberté d'expression, d'aller et venir, d'assemblée, d'association, et, plus largement, dans l'accès aux droits).

UN RISQUE INHÉRENT D'ATTEINTE AU DROIT AU RESPECT DE LA VIE PRIVÉE ET À LA PROTECTION DES DONNÉES

Consacrés par la Convention européenne des droits de l'homme (CEDH)[35] ainsi que par la Charte des droits fondamentaux de l'Union européenne[36], le droit au respect de la vie privée et le droit à la protection des données à caractère personnel visent à protéger l'autonomie et la dignité des individus[37], en les protégeant de toute intrusion injustifiée dans leur sphère privée. L'utilisation de technologies biométriques implique la collecte, la comparaison et/ou l'enregistrement de données dites sensibles dans un système informatique aux fins d'authentification, d'identification ou d'évaluation. Elle constitue dès lors une ingérence dans l'exercice de ces droits.

En effet, comme l'a jugé la Cour de justice de l'Union européenne (CJUE), « *l'image d'une personne enregistrée par une caméra constitue une donnée à caractère personnel [...] dans la mesure où elle permet d'identifier la personne concernée* »[38]. Au même titre, l'enregistrement vocal d'une personne contient nécessairement des données à caractère personnel. Comme l'explique la CNIL dans son Livre blanc sur les assistants vocaux, « *[l]a voix contient des marqueurs spécifiques à une personne, combinaisons de facteurs physiologiques et comportementaux. C'est ce qui en fait un attribut biométrique à part entière, qui peut être utilisé pour l'identifier* »[39]. De fait, les technologies biométriques réalisent des opérations de traitement de données à caractère personnel.

Pour être autorisées, celles-ci doivent en France respecter les grands principes et conditions strictes prévus par le Règlement général sur la protection des données (ci-après, RGPD)[40] et la loi Informatique et libertés[41]. Parmi les principes phares de ces textes figure l'interdiction de traitement de données dites « sensibles » dont font désormais partie les données biométriques, mais uniquement lorsqu'elles sont traitées aux fins d'identifier les personnes physiques de manière unique[42]. Un tel traitement ne peut être mis en œuvre, par exception, que dans certains cas particuliers, avec le consentement exprès des personnes, pour protéger leurs intérêts vitaux ou sur la base d'un intérêt public important, notamment[43]. De façon similaire, ce type de traitement ne peut être autorisé qu'en cas de nécessité absolue lorsqu'il est mis en œuvre à des fins policières, en vertu de dispositions issues de la directive « Police-Justice »[44].

Comme l'a relevé la CNIL, les traitements de données biométriques ne sont jamais tout à fait anodins[45]. Ils peuvent gravement porter atteinte au droit au respect de la vie privée comme à la protection des données. Largement documentés par les différentes autorités et instances européennes de protection des données[46], ces risques sont à apprécier *in concreto*, usage par usage, en tenant compte des finalités de chaque traitement. À l'instar des technologies de reconnaissance faciale, il convient effectivement de tenir compte du « *degré de contrôle des personnes sur leurs données personnelles, de leur marge d'initiative dans le recours à cette technologie, des conséquences qui en découlent pour elles (en cas de reconnaissance ou de non-reconnaissance) et de l'ampleur des traitements mis en œuvre* »[47] pour chaque technologie biométrique.

Il convient ainsi de distinguer les technologies dites actives où l'individu fournit volontairement des informations (par exemple, en plaçant son doigt sur un dispositif de contrôle) des technologies passives où les informations biométriques sont détectées, parfois à l'insu de la personne concernée. L'emploi de technologies biométriques actives d'authentification stockant les gabarits dans un support individuel à la libre disposition des personnes (carte à puce, smartphone, etc.) ne soulève pas les mêmes enjeux que celui d'une technologie biométrique passive stockant les gabarits qu'elle traite sur une base de données centralisée, en particulier lorsque cet usage vise à identifier des individus et qu'il se déroule à leur insu, sans avoir au préalable obtenu leur consentement.

Le développement et le déploiement sans fin de technologies de surveillance, vidéo-protection sur la voie publique, dans les transports publics, dans les parties communes des bailleurs sociaux, les magasins, à-travers le déploiement de caméras-piétons, de drones, s'accompagne en droit d'un assouplissement considérable 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. Ce phénomène est porteur de risques importants pour le respect de la vie privée comme l'a souligné le Défenseur des droits dans son avis n°20-13 du 21 décembre 2020[48]. Or, ces dernières années ont été marquées par une montée en puissance dans le monde entier des technologies biométriques passives employées à des fins d'identification. Cette évolution est largement contestée par de nombreux acteurs du monde associatif . Elle s'inscrit dans un mouvement plus large, dénoncé par le Défenseur des droits dès 2015, de recours trop facile à la technologie en dépit des risques pour les libertés publiques[50]. En Russie, des dispositifs de reconnaissance faciale automatisés ont été déployés sur la voie publique pour contrôler le respect des mesures sanitaires et lutter contre la propagation de l'épidémie de COVID-19[51]. Au Royaume Uni, il a été question de déployer ce même type de technologie pour vérifier le statut vaccinal des individus en combinant dispositif de reconnaissance faciale et passeport sanitaire, projet finalement abandonné suite aux mobilisations de la société civile[52]. Deux sociétés américaine et polonaise ont constitué des bases de données biométriques de grande ampleur à partir de photographies collectées massivement sur les profils de réseaux sociaux du monde entier dont elles vendent l'accès aux services de police, à des sociétés

privées et parfois même à des particuliers, leur permettant à partir d'une simple photographie de retrouver l'identité d'une personne à tout moment[53]. L'une d'entre elle a fait l'objet de sanctions de la part des autorités de protection des données suédoise[54] et canadienne[55] et est visée par de multiples procédures administratives en cours, y compris en France[56]. En Italie, l'autorité de protection des données a interdit l'utilisation du dispositif « SARI », un outil de reconnaissance faciale en temps réel déployé sur la voie publique afin d'identifier les étrangers en situation irrégulière[57].

Tandis que de tels usages sont encore au stade de l'expérimentation en France, les débats parlementaires et l'approche de la tenue des Jeux Olympiques de Paris en 2024 montrent une volonté d'adopter ce type de technologie. D'ores et déjà, la CNIL a eu l'occasion d'émettre de multiples avertissements suite aux déploiements de technologies biométriques d'identification parfois opérés au mépris de principes essentiels de la protection des données tels que les principes de licéité[60] et de proportionnalité[61].

Au regard du droit au respect de la vie privée et à la protection des données, ces pratiques alarment à raison, en particulier lorsque ces déploiements ne s'entourent nullement de garanties suffisantes.

En effet, plus les traitements de données biométriques reposant sur l'utilisation de bases de données se multiplient, plus le potentiel de voir survenir une faille de sécurité aux conséquences particulièrement graves pour les personnes concernées augmente[62]. Or, contrairement à un mot de passe, à un numéro de téléphone ou à une adresse postale, la divulgation non autorisée de données biométriques ne peut être corrigée. Ce type d'incident est déjà survenu[63]. Ces applications mettent en danger l'anonymat dans l'espace public en permettant une forme de surveillance généralisée, dans la mesure où elles permettent d'identifier instantanément et de pister les individus - ce risque a été rappelé par le Défenseur des droits dans son avis du 17 novembre 2020 sur la proposition de loi relative à la sécurité globale[64]. Ces problèmes surviennent essentiellement lorsque les acteurs agissent au mépris du droit applicable. Par exemple, concernant les usages privés de technologies biométriques, ceux-ci sont par principe interdits et doivent pouvoir justifier de l'une des exceptions de l'article 9 du RGPD. Or, trop souvent, aucune forme de consentement n'est collectée auprès des individus qui sont rarement informés de l'existence même des traitements.

Finalement, comme le soulevait un rapport réalisé sous l'égide de la rapporteuse spéciale de l'ONU sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, les développements technologiques, ainsi que la prolifération et la dépendance accrue à l'égard de diverses technologies destinées aux consommateurs, ont rendu les ingérences avec l'exercice du droit au respect de la vie privée à la fois moins perceptibles pour la société et les personnes concernées et, en même temps, plus intrusives, avec des conséquences potentiellement importantes, allant souvent au-delà du droit au respect de la vie privée[65].

UN POTENTIEL INÉGALÉ D'AMPLIFICATION ET D'AUTOMATISATION DES DISCRIMINATIONS

Parce qu'elles ciblent le plus souvent les caractéristiques des individus qui les exposent à des discriminations (origine, sexe, identité de genre, apparence physique, état de santé, handicap, âge..), les technologies biométriques (au-delà des marges d'erreurs d'allocation qui auront tendance à diminuer avec le rapide perfectionnement des systèmes) et la généralisation de leur usage sont susceptibles de perpétuer voire d'amplifier, pour certains groupes sociaux, les discriminations systémiques opérant au sein de la société.

ERREURS ET BIAIS AUX CONSÉQUENCES DISCRIMINATOIRES

Par définition, toute technologie biométrique est probabiliste et repose sur l'emploi d'algorithmes présentant un certain taux de faux-positifs comme de faux-négatifs[66].

Une technologie de reconnaissance des émotions affichées dans le cadre d'une procédure de recrutement peut déterminer à tort qu'un candidat est « nerveux » et lui assigner une note lui retirant toute chance d'être embauché. De façon similaire, un dispositif d'authentification par reconnaissance vocale déployé pour contrôler l'accès à un compte bancaire en ligne peut commettre une erreur dans la vérification de l'identité de la personne s'étant servie du dispositif. Enfin, un dispositif de reconnaissance faciale utilisé aux fins d'identifier les personnes faisant l'objet d'une interdiction de stade peut déterminer à tort qu'un supporter ne devrait pas assister à une rencontre sportive. **Les conséquences de ces erreurs varient en fonction des usages et peuvent aller du refus d'accès physique à un lieu ou à un événement à une arrestation erronée par les forces de l'ordre**[67].

En s'intéressant de près aux profils des personnes victimes de ces erreurs, de nombreuses études ont démontré dès 2018 qu'il s'agissait majoritairement de personnes issues de groupes discriminés et/ou vulnérables (femmes, enfants mineurs, personnes transsexuelles, personnes à la peau foncée, entre autres)[68] en raison des biais discriminatoires des algorithmes sur lesquels reposent ces technologies. Comme l'expliquait le Défenseur des droits en 2020, ces biais peuvent provenir aussi bien du manque de représentativité des données mobilisées dès la phase d'apprentissage des algorithmes[69] que de l'intégration, après traduction mathématique, de pratiques et comportements passés discriminatoires et des discriminations systémiques opérant au sein de la société[70].

De manière significative, qu'il s'agisse de dispositifs d'authentification, d'identification ou d'évaluation, lorsqu'une technologie biométrique est déployée dans un espace visité par des millions d'individus comme un aéroport ou une gare, même un très faible taux de faux positifs et de faux négatifs[71] implique que des centaines d'individus subissent les erreurs de ces systèmes et les conséquences de telles erreurs[72].

Ainsi, si les systèmes d'authentification, notamment de reconnaissance faciale, peuvent proposer des taux de précision atteignant 99,5%[73], ces 0,5% restants peuvent représenter une multitude d'individus exposés à un traitement inégal. Toutes les erreurs ne trouvent pas leur source dans des biais discriminatoires. À cet égard, la mise en place de voie alternative peut constituer une solution mais elle ne saurait justifier le maintien d'atteintes au principe de non-discrimination.

En effet, indépendamment des voies alternatives proposées comme dans le cadre du dispositif Alicem[74], les effets discriminatoires des algorithmes ne sauraient être ignorés : **si les taux d'erreur restent importants pour certaines catégories de personnes protégées par le droit de la non-discrimination, elles seront lésées et devront systématiquement prendre la voie alternative (qui, de fait, ne sera plus vraiment alternative)**. Or, compte tenu de la nature probabiliste de ces systèmes, ceux-ci ne permettent guère d'atteindre un taux d'erreur qui serait nul : il restera toujours un pourcentage infime de faux positifs et de faux négatifs. Afin d'éviter toute discrimination, le taux d'erreur devrait être décorrélé des catégories protégées. Pour ce faire, les jeux de données non représentatifs sur lesquels les algorithmes d'authentification sont entraînés peuvent être la source des biais et doivent donc être corrigés. Afin d'assurer une plus grande fiabilité des algorithmes de reconnaissance faciale dont nous avons vu les biais concernant les femmes et personnes à la peau foncée, les profils et données devraient notamment être plus variés pour refléter la diversité de la population réelle et assurer un bon entraînement de l'algorithme sur des profils minoritaires.

Par ailleurs, un système qui vise à authentifier un individu n'est pas automatiquement un dispositif atteignant les meilleurs taux de précision dans la mesure où ceux-ci dépendent de plusieurs facteurs (éclairage, qualité d'image, etc.). Aujourd'hui encore certains dispositifs d'authentification commettent de nombreuses erreurs aux conséquences discriminatoires que l'on ne saurait tolérer du simple fait que leur fonctionnement serait respectueux du droit des données personnelles[75].

Pour autant, le contrôle que maintiennent les personnes sur les dispositifs d'authentification permet à celles-ci de prendre conscience des erreurs qui surviendraient : la vérification d'identité de la personne n'a pas fonctionné, elle est immédiatement invitée à réitérer son essai et/ou à faire usage d'une voie alternative. Cela n'est pas toujours le cas lorsque les technologies biométriques sont utilisées aux fins d'identification comme d'évaluation.

Quand elles sont déployées dans des lieux accessibles au public, les technologies biométriques d'identification et d'évaluation ne permettent pas aux personnes de s'opposer à leur utilisation ou de leur préférer une voie alternative : les données biométriques de chaque passant sont traitées de manière indifférenciée. C'est le cas notamment des technologies de reconnaissance faciale « en temps réel » déployées aux fins d'identifier des personnes recherchées. Or, la précision de ce type de système est nettement inférieure à celle des dispositifs d'authentification[76], ce qui est particulièrement inquiétant lorsqu'ils sont utilisés à des fins policières. En effet, outre les défauts de qualité de la source des images collectées et comparées, ces erreurs trouvent souvent leurs origines dans des biais discriminatoires, les données d'entraînement des algorithmes de reconnaissance faciale souffrant encore aujourd'hui d'un manque prononcé de représentativité[77]. Par exemple, de tels usages peuvent avoir pour conséquence que certaines personnes se retrouvent arrêtés à tort plus fréquemment en raison de leur couleur de peau[78]. Aux États-Unis, trois hommes noirs ont ainsi déjà été emprisonnés injustement suite aux erreurs de systèmes de reconnaissance faciale[79]. Au Royaume Uni, une étude dédiée à l'utilisation de reconnaissance faciale aux fins d'identification par les services de police de Londres a déterminé que sur 22 individus interpellés sur la base d'une concordance établie par ordinateur et jugée crédible par un opérateur humain, quatorze de ces concordances (soit 63,64%) se sont révélées incorrectes et seulement huit (soit 36,36%) correctes[80]. L'utilisation de ce type de dispositif par les services de police britanniques a par ailleurs donné lieu à la première décision judiciaire d'envergure sur le sujet en 2020 : la Cour d'appel de Londres a conclu que les services de police ne s'étaient pas suffisamment assurés de l'absence de biais discriminatoires du logiciel utilisé quant à l'origine ethnique ou au genre des personnes qu'il visait à identifier[81], les risques de discrimination découlant de l'utilisation même des outils biométriques.

LES RISQUES DE DISCRIMINATION DÉCOULANT DE L'UTILISATION MÊME DES OUTILS BIOMÉTRIQUES

Le débat public sur la précision des technologies biométriques est important, notamment dans la mesure où les biais de ces systèmes peuvent entraîner comme nous l'avons mentionné des situations discriminatoires, mais il a trop longtemps occulté une autre réalité. En effet, **même avec un taux de précision avoisinant les 100%, l'utilisation d'outils biométriques d'identification et d'évaluation peut être génératrice de discriminations. Pire, elle peut les amplifier**.

Dans une enquête de 2017 dédiée aux relations police/population, le Défenseur des droits relevait que les contrôles d'identité ciblent particulièrement certaines zones territoriales et donnent lieu à de fortes pratiques discriminatoires fondées sur l'origine, suggérant un profilage racial et social des opérations de contrôle sur des hommes jeunes, perçus comme noirs ou arabes/maghrébins. Alors que plus de 80% des hommes enquêtés déclarent n'avoir fait l'objet d'aucun contrôle d'identité au cours des 5 dernières années, « 80% des personnes correspondant au profil de "jeune homme perçu comme noir ou arabe" déclarent avoir été contrôlées dans les cinq dernières années (contre 16% pour le reste des enquêtés) ». Ces profils ont donc vingt fois plus de probabilités d'être contrôlés[82].

Si demain les services de police pouvaient mener ces contrôles à l'aide de dispositifs biométriques d'identification et/ou d'évaluation couplés à des méthodes de verbalisation à distance[83], le risque d'un déploiement concentré dans des zones géographiques où les jeunes hommes perçus comme arabes/maghrébins ou noirs sont surreprésentés pourrait démultiplier les situations discriminatoires avec des contrôles instantanés de centaines d'individus effectués à raison de leur sexe, de leur origine, de leur âge et/ou de leur situation économique. Ces craintes ne sont pas sans fondement quand on considère, d'une part, les développements de ces technologies à des fins sécuritaires (c'est le cas par exemple du déploiement dans certains territoires de drones de surveillance pendant la période de confinement), d'autre part, les ciblages discriminatoires par certains services de police qui ont déjà fait l'objet de décisions judiciaires et d'observations du Défenseur des droits qui relevait le climat d'exclusion et de discrimination qu'ils pouvaient entretenir[84]. Comme c'est aujourd'hui le cas dans le domaine des infractions routières (notamment le stationnement des personnes en situation de handicap[85]), la verbalisation à distance pourrait ne pas prendre en compte les spécificités des situations particulières des personnes. De plus, le développement des villes dites « intelligentes » permis par le couplage de la vidéo et des technologies d'identification et d'évaluation présente des risques de discrimination : en repérant des personnes sans abri ou se livrant à la mendicité, les villes sont à même de dépêcher un accompagnement social adapté sur les lieux concernés comme de stigmatiser et discriminer ces personnes en situation de particulière vulnérabilité. Si la Commission européenne a récemment proposé d'interdire par principe l'utilisation de dispositifs d'identification à distance sur la voie publique à des fins policières, de nombreuses exceptions ont été aménagées laissant à la libre appréciation des États Membres le choix d'utiliser ou non ce type de dispositif, par exemple, lorsqu'une infraction est punie d'une peine d'au moins trois ans d'emprisonnement[86]. Les niveaux de confiance dans la police ne dépendent pas seulement du contrôle en lui-même, mais aussi du fait qu'il soit perçu ou non comme du profilage racial[87]. Aussi, l'utilisation d'outils biométriques d'identification et/ou d'évaluation par les forces de police pourrait dégrader la relation police/population si elle ne s'entoure pas de garanties suffisantes.

Dans le cadre de la lutte contre l'immigration illégale en Europe, l'Union européenne finance depuis 2016 un projet appelé iBorderCtrl[88] : le voyageur étranger désireux d'entrer dans l'espace européen doit passer par un "détecteur de mensonges par reconnaissance faciale" qui le redirige selon les résultats soit dans des files d'attente rapides ou au contraire vers des contrôles poussés[89].

Ce système a été testé aux frontières terrestres de l'UE en Hongrie, en Lettonie et en Grèce. De nombreuses associations ont dénoncé une technologie hautement expérimentale, dont les résultats ne sont pas fiables et visent des personnes en situation de particulière vulnérabilité[90].

De façon générale, le risque de voir survenir des discriminations ne saurait se réduire au contexte policier. Il concerne également les usages relevant du secteur privé, en particulier en matière d'évaluation. L'utilisation de dispositifs de détection des traits de personnalité d'un individu dans le cadre de procédures de recrutement aux fins d'analyser des entretiens et d'automatiquement assigner des scores aux différents candidates et candidats en fonction de leur soi-disant personnalité est particulièrement éloquente[91]. Ces systèmes peuvent engendrer des discriminations importantes, en particulier pour les candidates et les candidats en situation de handicap : si les caractéristiques de leurs visages ou leurs manières de se tenir et/ou de s'exprimer diffèrent de la norme et donc de l'écrasante majorité des données sur lesquelles les algorithmes de recrutement ont été entraînés pour assigner des scores, ces personnes risquent de ne pas voir leurs aptitudes à exercer un poste reconnues, même si leurs traits de personnalité seraient tout aussi bénéfiques à l'exercice de ce poste que ceux d'une personne dite valide[92]. Comme le soulignait Laurence Devillers, professeure en intelligence artificielle à la Sorbonne Université, « il y a une dimension culturelle énorme dans notre façon de nous exprimer. Que fait-on des personnes bègues, de celles qui s'expriment naturellement lentement, de celles qui ont un accent ? »[93]. Par ailleurs, ces systèmes peuvent être directement discriminants, en détectant notamment des faiblesses psychologiques ou des problèmes mentaux qui relèvent des critères de discrimination de l'état de santé.

Récemment, une grande entreprise américaine spécialisée dans ce mode de recrutement annonçait renoncer aux usages d'évaluation tirée de l'analyse vidéo du visage des candidats pendant les entretiens. Pour autant, l'analyse automatisée de leur intonation comme de leur comportement a été maintenue alors même que déceler les émotions dans la voix ou la signification d'un silence reste très aléatoire comme le relèvent les spécialistes[94].

Si leur adoption est encore limitée en France, certaines entreprises de recrutement commercialisent déjà des logiciels réduisant les opportunités des personnes sans que leur efficacité[95] ne soit clairement documentée et auditée de manière indépendante. Ces développements s'effectuent parfois au mépris du droit du travail qui prévoit une obligation de pertinence s'agissant des informations recueillies par le recruteur. Celles-ci doivent en effet présenter un lien direct et nécessaire avec l'emploi proposé ou avec l'évaluation des aptitudes professionnelles[96]. Une association de professionnels a appelé à exclure des techniques de recrutement toute donnée n'ayant aucun caractère prédictif fiable et avéré sur la réussite des candidates et des candidats[97].

L'EFFET DISSUASIF

L'une des singularités des technologies biométriques d'identification et d'évaluation lorsqu'elles sont déployées dans des lieux publics repose sur l'effet dissuasif qu'elles peuvent avoir pour l'exercice de droits fondamentaux comme la liberté d'expression, d'aller et venir, d'assemblée, d'association, et, plus largement, l'accès aux droits.

Le Contrôleur européen de la protection des données, Wojciech Wiewiórowski a pointé ces risques même lorsque ces technologies correspondent à des fins légitimes et d'intérêt public. Le fait qu'elles fonctionnent souvent à l'insu des personnes concernées et sans contrôle de leur part (ce que l'on appelle l'absence de friction) tend à dissuader les personnes d'exercer leurs droits, et ce peu importe l'envergure de leur déploiement, la peur de la surveillance étant suffisante pour affecter notre comportement[98]. L'un des aspects nécessaires dans l'exercice de ces libertés repose effectivement sur l'anonymat de groupe[99], en l'absence duquel les individus peuvent être amenés à altérer leur comportement et à ne pas exprimer leurs pensées de la même manière[100].

En France, récemment encore, s'agissant de l'élargissement du recours aux drones par les services de police prévu par la « loi pour une sécurité globale préservant les libertés », le Conseil constitutionnel relevait dans le sillage de la CNIL[101] que ces appareils sont « *susceptibles de capter, en tout lieu et sans que leur présence soit détectée, des images d'un nombre très important de personnes et de suivre leurs déplacements dans un vaste périmètre* »[102], insistant sur la nécessité d'assortir la mise en œuvre de ces systèmes de surveillance de garanties particulières. Tel était le sens de l'avis 20-05 du Défenseur des droits[103] comme de celui du Conseil des droits de l'homme de l'ONU, qui, dans un rapport exprimait ses préoccupations sur l'usage de drones avec caméras, « *susceptible d'avoir un effet dissuasif sur des individus qui se trouvent dans l'espace public* »[104].

Par analogie, les technologies biométriques d'identification à distance sont tout autant, si ce n'est plus, intrusives encore. Le Conseil constitutionnel a d'ailleurs maintenu l'interdiction explicite du traitement des images des drones par des logiciels de reconnaissance faciale[105].

Enfin, l'effet dissuasif des technologies biométriques se traduit également par un risque d'exclusion, en particulier pour les personnes issues de groupes particulièrement discriminés comme les étrangers. Dans un rapport, la Rapporteuse spéciale de l'ONU sur les formes contemporaines de racisme, Tendayi Achiume, soulignait que l'utilisation de technologies biométriques pouvait priver les réfugiés et les demandeurs d'asile de l'accès aux services de base essentiels, de par leur effet dissuasif[106]. De peur d'être identifiés en tant que « sans papier », certains migrants pourraient notamment renoncer aux soins de santé auxquels ils ont pourtant légalement droit, même en cas d'urgence.

LE CAS PARTICULIER DES MINEURS

En France comme ailleurs, les enfants à l'instar des adultes sont de plus en plus exposés aux technologies biométriques, mais avec sans doute un risque plus fort de banalisation pour une génération née et acculturée à ces nouvelles technologies sans en connaitre les risques et limites par ailleurs. Ce phénomène n'est pas nouveau. Dès l'an 2000, la CNIL avait émis un avis défavorable concernant l'installation d'un système d'authentification conditionnant l'accès à la cantine d'un collège à l'utilisation d'une base de données d'empreintes digitales[107].

Le principe de responsabilité du RGPD ayant mis fin à l'obligation pour les établissements scolaires d'obtenir une autorisation pour mettre en place ce type de solution biométrique[108] en 2018, il appartient désormais

à ces derniers de s'assurer qu'ils respectent le droit applicable et documentent leurs activités de traitement.

L'introduction de technologies biométriques plus récentes dans les enceintes scolaires a donné lieu à des avertissements et sanctions en Europe. En Suède, l'autorité de protection des données a ainsi sanctionné une école qui avait déployé un dispositif de reconnaissance faciale afin d'identifier les élèves pour vérifier leur présence[109]. En France, la CNIL a considéré que l'expérimentation visant à équiper l'entrée de deux lycées de portiques de reconnaissance faciale afin d'identifier les élèves de chaque établissement et de refuser le passage aux personnes ne les fréquentant pas contrevenait aux principes de proportionnalité et de minimisation des données posés par le RGPD[110]. Dans les deux cas, les autorités ont considéré que le consentement obtenu n'était pas valide et que le recours aux dispositifs de reconnaissance faciale était disproportionné compte tenu de l'existence de moyens nettement moins intrusifs comme un contrôle par badge.

Les données personnelles des enfants font l'objet d'un encadrement rigoureux par le RGPD comme par la loi Informatique et Libertés qui leur octroient une protection spécifique[111]. Celui-ci découle de l'article 24 de la Charte des droits fondamentaux de l'Union européenne qui prévoit que dans tous les actes relatifs aux enfants, qu'ils soient accomplis par des autorités publiques ou des institutions privées, l'intérêt supérieur de l'enfant doit être une considération primordiale.

Or, le déploiement de technologies biométriques d'identification et d'évaluation à distance sur la voie publique va à l'encontre de ces protections dans la mesure où ces systèmes collectent de manière généralisée et indifférenciée les données biométriques de chaque personne entrant dans leur champ d'opération, enfants compris. Quand bien même ces données peuvent par la suite être supprimées rapidement voire instantanément, leur simple traitement représente un risque d'atteinte grave aux droits de l'enfant. Comme l'Agence européenne des droits fondamentaux le relevait en 2018, lorsque la reconnaissance faciale est utilisée pour prévenir, détecter et enquêter sur le terrorisme et d'autres crimes graves, il est difficile de voir comment cela peut justifier le traitement d'images faciales d'enfants n'ayant pas atteint l'âge de la responsabilité pénale[112].

Le Défenseur des droits, dans sa double mission de défense et de promotion de l'intérêt supérieur et des droits des enfants, restera vigilant à ce que ces droits soient préservés.

RECOMMANDATIONS

Les avancées que permettent les technologies biométriques ne sauraient s'effectuer ni au détriment d'une partie de la population, ni au prix d'une surveillance généralisée. Comme l'a déjà rappelé le Défenseur des droits, le droit de la non-discrimination doit être respecté en toutes circonstances, y compris lorsqu'une décision implique le recours à un algorithme[113]. De même, l'accès aux droits doit rester garanti pour toutes et tous.

Pourtant, l'augmentation récente du nombre de décisions de différentes autorités de protection des données européennes sanctionnant l'utilisation de dispositifs biométriques, en particulier de reconnaissance faciale[114], témoigne d'une multiplication des usages effectués en violation du droit applicable. Le principe de responsabilité du RGPD doublé du manque de moyens humains et financiers des autorités[115] porte d'ailleurs à croire que ces violations sont probablement bien plus nombreuses que celles ayant été recensées.

Le droit des données personnelles apporte une première réponse au déploiement de ces technologies en encadrant strictement leur usage à travers les grands principes de nécessité, de conservation limitée et de minimisation des données ou via la protection spécifique apportée aux données les plus sensibles. Dans les recours en discrimination, il constitue un point d'appui utile. Pour autant, il n'est parfois pas suffisamment développé pour lutter efficacement contre les discriminations, en particulier contre les discriminations de groupes[116]. À titre d'exemple, l'article 95 de la loi Informatique et libertés interdit tout profilage qui entrainerait une discrimination à l'égard d'une personne physique sur la base de données sensibles. Or, la liste des données dites sensibles ne recoupe pas exactement la liste des critères prohibés de discrimination de la loi du 27 mai 2008[117]. La question de l'égalité des sexes ou de la discrimination fondée sur le sexe est d'ailleurs totalement absente du RGPD pour lequel ni le genre ni le sexe ne sont considérés comme des catégories particulières de données[118]. De façon similaire, les données biométriques ne sont considérées comme des données sensibles que lorsque leur traitement vise à identifier les personnes de manière unique. Dès lors, les traitements effectués aux fins d'évaluer les individus ne bénéficient guère de cette protection renforcée. Par ailleurs, les proxies et corrélations de données « non-sensibles » peuvent aboutir aux mêmes effets discriminatoires que les traitements portant sur ces catégories particulières de données.

Aussi, se concentrer sur l'impact des technologies biométriques sur le droit à la vie privée et à la protection des données est nécessaire mais insuffisant pour appréhender l'effet global sur les droits fondamentaux[119]. À cet égard, la CNIL a d'ailleurs elle-même à plusieurs reprises mis en avant la nécessité de soupeser les atteintes à de nombreux autres droits[120].

Comment identifier une discrimination lorsqu'elle est le fruit d'un outil biométrique dont on ignore l'utilisation et/ou les biais ? Comment s'assurer que les finalités d'usage d'une telle technologie ne seront pas détournées à des fins discriminatoires ? Comment éviter l'avènement d'une forme de surveillance généralisée obstruant l'accès aux droits, en particulier pour les plus démunis ? Comment garantir que les atteintes aux droits fondamentaux engendrées par des outils biométriques puissent être sanctionnées ?

Avant de multiplier les expérimentations, il apparaît essentiel d'être en mesure de répondre à chacune de ces questions. La récente proposition de règlementation de l'intelligence artificielle de la Commission européenne[121] et les lignes directrices du Conseil de l'Europe sur la reconnaissance faciale[122] apportent des indications.

Dans le cadre de ses missions de lutte contre les discriminations et de promotion de l'égalité, de respect de la déontologie par les personnes exerçant des activités de sécurité et de

défense et de promotion de l'intérêt supérieur et des droits de l'enfant, le Défenseur des droits souhaite adresser un certain nombre de recommandations pour assurer le respect des droits fondamentaux à l'ère des technologies biométriques.

ÉCARTER LES MÉTHODOLOGIES D'ÉVALUATION NON PERTINENTES

Aujourd'hui, il apparaît essentiel d'interroger systématiquement l'utilité des technologies biométriques en amont de leur déploiement, y compris dans le cadre d'expérimentations. Ce questionnement devrait s'opérer tant de la part des vendeurs de ces « solutions » qui gagneraient à davantage interroger les usages des produits qu'ils conçoivent, que de la part des acquéreurs qui devraient faire preuve d'esprit critique à l'égard des applications qui leur sont vendues. Dès lors qu'il n'est pas possible scientifiquement de déduire des traits de personnalité de la simple apparence, de l'intonation ou du comportement d'une personne, ces derniers ne devraient pas céder à la facilité ou aux gains de temps et d'argent que promet l'adoption de certaines technologies d'évaluation.

Compte tenu du risque de multiplication des situations discriminatoires qu'implique l'utilisation de ces outils biométriques, le Défenseur des droits en appelle à la responsabilisation des acteurs. En matière d'embauche, par exemple, il convient de rappeler que l'article L122-1-8 du Code du travail précise que « [l]es méthodes et techniques d'aide au recrutement ou d'évaluation des candidats à un emploi doivent être pertinentes au regard de la finalité poursuivie ».

Le déploiement de technologies fondées sur des méthodologies non éprouvées scientifiquement préoccupe le Défenseur des droits. Ce déploiement dépasse le champ de l'emploi comme l'ont relevé le Contrôleur Européen de la Protection des Données et le Comité Européen de la Protection des Données qui préconisent l'interdiction générale des méthodes d'évaluation des émotions[123].

METTRE EN PLACE DES GARANTIES FORTES ET EFFECTIVES POUR S'ASSURER DU RESPECT DES DROITS DES INDIVIDUS

Le déploiement de tout dispositif biométrique ne saurait s'effectuer sans satisfaire des conditions strictes de nécessité et de proportionnalité eu égard à la gravité des ingérences causées.

USAGES À DES FINS POLICIÈRES

Dans le contexte policier, les mesures utiles à la prévention de la criminalité ne sauraient porter une atteinte inappropriée à d'autres droits, nécessaires au bon fonctionnement d'une société démocratique, tels que le droit à la vie privée, le droit à la liberté d'expression, de réunion et d'association et le droit à la non-discrimination. Conformément à l'article 10 de la directive police-justice, le déploiement d'outils biométriques d'identification ne peut être autorisé qu'en cas de nécessité absolue. Si cette notion s'apprécie « *au regard des seules nécessités de l'intervention au cours de laquelle [les données sensibles] sont collectées, notamment pour la compréhension d'un fait ou la qualification ultérieure d'une infraction* »[124], elle doit être évaluée en même temps que la proportionnalité à la finalité et que son impact sur les droits des personnes concernées[125]. En d'autres termes, il conviendrait de tenir compte des analyses d'impact effectuées afin d'identifier de potentielles atteintes aux droits fondamentaux des individus avant toute utilisation du dispositif, mais aussi de systématiquement s'interroger sur l'opportunité de faire usage d'un moyen d'identification alternatif qui serait moins intrusif. En tout état de cause, le recours à l'identification biométrique ne saurait concerner tout type d'infraction.

S'agissant des usages les plus intrusifs à l'instar des dispositifs biométriques d'identification à distance en temps réel dans les lieux publics, il apparaît difficile de concevoir comment l'utilisation de ces systèmes pourrait être considérée comme nécessaire et proportionnée à ce jour compte tenu des risques significatifs de détournement

d'usage qu'ils représentent, c'est-à-dire des risques de voir ces dispositifs utilisés pour des finalités de traitement distinctes de celles pour lesquelles ils ont été déployés[126], et des biais qu'ils comportent à l'égard des groupes discriminés[127]. Récemment, le Contrôleur Européen de la Protection des Données et le Comité Européen de la Protection des Données appelaient conjointement à prohiber toute utilisation de technologies de reconnaissance automatisée des caractéristiques humaines dans les espaces accessibles au public[128].

Dans la mesure où le législateur a explicitement interdit le recours à l'utilisation de logiciels de reconnaissance faciale dans le cadre de la captation d'images par drones des forces de police[129], le Défenseur des droits soutient que cette interdiction devrait logiquement être étendue à l'intégration de technologies de reconnaissance faciale aux systèmes de surveillance existants (caméras piétons, de vidéosurveillance, etc.). Si le législateur en venait à autoriser ces technologies, leur utilisation devrait *a minima* se limiter strictement aux infractions les plus graves et faire l'objet d'autorisations spécifiques, limitées dans le temps comme dans l'espace, et délivrées au cas par cas par la CNIL ou une autorité de certification compétente (par exemple, celle prévue par la proposition de règlement sur l'IA de la Commission européenne), ou par une autorité judiciaire.

TOUT USAGE CONFONDU

Quelle que soit la nature de l'usage, qu'il s'agisse d'authentification, d'identification ou d'évaluation, une attention particulière doit être portée au respect du principe de non-discrimination.

Les biais discriminatoires des technologies biométriques doivent être contrôlés à chaque étape de déploiement. Des taux de fiabilité et de précision minimales des algorithmes utilisés doivent être fixés et respectés, en particulier s'agissant des personnes issues de groupes protégés. Le droit au recours des personnes victimes de discriminations doit être assuré et facilité par l'entité publique comme privée responsable du traitement. Conditionner l'accès aux services publics à l'utilisation de technologies biométriques d'identification viole le droit d'accès des usagers, quand bien même ces dispositifs seraient très précis[130]. Pour le Défenseur des droits, la réalisation des démarches administratives dématérialisées doit demeurer une possibilité ouverte à l'usager et non devenir une obligation[131]. Enfin, même si le recueil et le traitement de données sensibles est déjà strictement encadré, le Conseil de l'Europe préconise qu'en matière de reconnaissance faciale, l'utilisation de technologies biométriques dans le seul but de déterminer la couleur de peau d'une personne, ses croyances religieuses ou ses convictions philosophiques ou politiques, son sexe, son origine raciale ou ethnique, son âge, son état de santé ou sa condition sociale soit explicitement interdite à moins que des garanties appropriées ne soient prévues par la loi pour éviter tout risque de discrimination[132].

REPENSER LES CONTRÔLES EXISTANTS

Alors que certaines des technologies biométriques les plus récentes peuvent opérer à distance et à l'insu des individus, la garantie d'une voie alternative à leur utilisation mobilisable en matière d'authentification et soulignée par la jurisprudence Alicem du Conseil d'Etat[133] n'apparaît plus adaptée. En effet, ces technologies s'appliquent automatiquement à chacun de manière indifférenciée. Par conséquent, contrairement aux usages ayant pour finalité l'authentification des personnes, en matière d'identification et d'évaluation sur la voie publique, deux parcours parallèles paraissent difficilement envisageables. Comment dès lors anticiper le risque de voir survenir des situations discriminatoires et d'obstruction dans l'accès aux droits ? Le Défenseur des droits appelle à imaginer de nouveaux mécanismes de contrôle permettant d'encadrer ces usages.

Trop souvent, les contrôles des dispositifs biométriques se limitent aux normes de cybersécurité et de protection de la vie privée alors qu'ils devraient prendre en compte d'autres exigences telles que la lutte contre les biais discriminatoires ou le respect du droit des mineurs.

Les analyses d'impact relatives à la protection des données imposées par l'article 35 du RGPD font référence au risque élevé que peut engendrer un traitement pour les droits et libertés des personnes physiques. Cette analyse préalable, obligatoire en matière de technologie biométrique, doit contenir une évaluation des risques pour les droits et libertés des personnes et constitue donc déjà un moyen d'anticiper des effets discriminatoires. Les acteurs se limitent néanmoins dans le cadre des analyses d'impact, lorsqu'elles sont réalisées, aux seuls droits que garantit le RGPD aux personnes concernées (rectification des données personnelles, effacement, portabilité, opposition, notamment). Comme le Défenseur des droits l'avait déjà souligné dans sa déclaration de mai 2020, les enjeux des risques discriminatoires, dont nous avons souligné l'importance s'agissant des outils biométriques, ne sont donc pas explicitement intégrés[134].

De façon similaire, dans le cadre des grands projets informatiques de l'État, le décret du 25 octobre 2019[135] prévoit une obligation d'évaluation préalable des systèmes d'information par la Direction interministérielle du numérique (Dinum) lorsqu'un marché public dépasse la somme de 9 millions d'euros et aménage une série d'exceptions[136]. Néanmoins, ce nouveau contrôle n'intègre aucun paramètre propre au respect des droits et libertés. 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.

Pour ce faire, il invite le législateur à s'inspirer largement de la proposition de réglementation de l'intelligence artificielle de la Commission européenne. Celle-ci prévoit notamment l'obligation pour les fournisseurs de dispositifs biométriques d'identification à distance de respecter certaines exigences strictes en terme de transparence et d'évaluation des risques avant toute mise en service et/ou commercialisation de ces systèmes ainsi qu'une procédure d'évaluation de conformité *ex-ante*[137].

Par ailleurs, les analyses d'impact prévues par le RGPD peuvent être aujourd'hui effectuées en toute autonomie par les responsables de traitement au titre du principe de responsabilité et donc possiblement « orientées ». À cet égard, la proposition de la Commission européenne prévoit que les dispositifs d'identification biométrique à distance auront pour obligation de recourir à un audit externe et indépendant de leur conformité[138]. Pour le Défenseur des droits, une telle obligation devrait être étendue à l'ensemble des dispositifs d'évaluation et de catégorisation biométriques.

Enfin, les biais algorithmiques pouvant apparaitre au-delà de l'étape de l'évaluation préalable des outils, le Défenseur des droits rappelle sa recommandation en faveur d'un contrôle régulier des effets des algorithmes après leur déploiement sur le modèle du contrôle des effets indésirables des médicaments[139]. À cet égard, la CNIL estime que dans un contexte d'évolution technologique et en vue d'assurer un niveau de risque acceptable, il est nécessaire de prévoir une analyse d'impact de manière régulière[140]. Pour sa part, la Commission européenne a proposé la mise en place d'un système de contrôles à mettre en œuvre tout au long du cycle de vie des dispositifs[141].

NOTES

[1] Rapport de la CNIL, « Reconnaissance faciale : pour un débat à la hauteur des enjeux », novembre 2019 ; voir également CNIL, « Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position » Octobre 2019 ; CNIL, « La CNIL appelle à la vigilance sur l'utilisation des caméras dites « intelligentes » et des caméras thermiques », Juin 2020 ; CNIL, « Caméras dites « intelligentes » et caméras thermiques : les points de vigilance de la CNIL et les règles à respecter », Juin 2020.

[2] Déclaration du Défenseur des droits, « Algorithmes, prévenir l'automatisation des discriminations », mai 2020.

[3] Commission Nationale de l'Informatique et des Libertés, Biométrie.

[4] Contrôleur européen de la protection des données, « 14 misunderstandings with regard to identification and authentication », juin 2020

[5] Thales, "Biometrics: definition, use cases and latest news".

[6] *Ibid*, p.1.

[7] Castelluccia, Claude, Le Métayer, Daniel. Analyse des impacts de la reconnaissance faciale – Quelques éléments de méthode. [Rapport de recherche] Inria Grenoble Rhône-Alpes, 2019.

[8] « Passage Automatisé Rapide Aux Frontières Extérieures ».

[9] Ministère de l'Intérieur, « Passez les contrôles aux frontières plus rapidement », Juillet 2019.

[10] Celle-ci peut être issue tant d'une photographie que d'une vidéo, y compris en direct. On parle alors de reconnaissance faciale ou comportementale « en temps réel ».

[11] Commission Nationale de l'Informatique et des Libertés, Définition, Reconnaissance faciale.

[12] T. Kinnunen, E. Karpov and P. Franti, « Real-time speaker identification and verification », in IEEE Transactions on Audio, Speech, and Language Processing, vol. 14, no. 1, pp. 277-288, Janvier 2006, doi: 10.1109/TSA.2005.853206.

[13] O. Costilla-Reyes, R. Vera-Rodriguez, P. Scully and K. B. Ozanyan, « Analysis of Spatio-Temporal Representations for Robust Footstep Recognition with Deep Residual Neural Networks », in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 41, no. 2, pp. 285-296, Février 2019, doi: 10.1109/TPAMI.2018.2799847.

[14] Commission européenne, Proposal for a Regulation laying down harmonised rules on artificial intelligence, avril 2021, p. 19.

[15] Données sensibles au sens de l'article 6 de la loi Informatique et Libertés (données révélant directement ou indirectement l'origine raciale ou ethnique des personnes, les opinions politiques, les convictions religieuses ou philosophiques, ou encore l'appartenance syndicale notamment).

[16] *Ibid*.

[17] Sur la base du croisement entre les images des personnes présentes dans le périmètre de l'événement et une liste de personnes recherchées. Par exemple, voir l'avertissement de la CNIL sur le déploiement de la reconnaissance faciale dans le stade du FC Metz.

[18] C'est le cas du traitement d'antécédents judiciaires (TAJ) en France, utilisé, en application des articles 230 6 à 230-11 du code de procédure pénale, dans le cadre des enquêtes judiciaires afin de faciliter la constatation des infractions, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs.

[19] De telles technologies ont notamment été utilisées par la police du Pays de Galles du Sud, « Facial recognition use by South Wales Police ruled unlawful ».

[20] C'est le cas du système de reconnaissance faciale SARI en Italie, « Italy : Interior ministry's facial recognition system is unlawful » ; « Riconoscimento facciale: Sari Real Time non è conforme alla ».

[21] Commission européenne, Proposal for a Regulation laying down harmonised rules on artificial intelligence, avril 2021, p. 42.

[22] *Ibid*, p.42 ; voir également Avis du groupe de travail « article 29 » sur la protection des données n°3/2012 sur l'évolution des technologies biométriques, p.6

[23] Certaines entreprises proposent d'assigner automatiquement un score « d'employabilité » aux candidates et aux candidats à un recrutement en fonction de leur vitesse de diction, du choix des mots qu'ils ou elles utilisent et/ou des mouvements de leurs visages au cours d'un entretien vidéo. Voir en ce sens : « Votre entretien d'embauche sera peut-être jugé par une IA », *Numerama*, Mai 2020.

[24] Certains systèmes de lutte contre la fraude aux examens administrés à distance affirment pouvoir automatiquement identifier les comportements suspects des étudiantes et des étudiants en suivant le mouvement de leurs yeux et de leurs têtes, en enregistrant le son de la pièce où ils ou elles se trouvent et en analysant les mouvements de souris et de clavier. Voir en ce sens : Feathers & Rose, « Students are Rebelling Against Eye-Tracking Exam Surveillance Tools », *Vice*, Septembre 2020.

[25] En analysant les mouvements du visage d'un conducteur ou d'une conductrice et en en déduisant des signes de fatigue à partir de la vitesse de clignement des yeux ou de la présence de bâillements par exemple. Voir en ce sens : Elgan, « What happens when cars get emotional », *Fast Company*, Juin 2019.

[26] Par exemple, en analysant la démarche des personnes présentes dans un magasin, certains systèmes affirment pouvoir calculer leur propension à commettre des vols. Voir en ce sens : Wiggers, « Cashierless tech could detect shoplifting, but bias concerns abound », *Venturebeat*, Janvier 2021.

[27] Italie, Garante per la protezione dei dati personali, Installazione di apparati promozionali del tipo « digital signage » (definiti anche Totem) presso una stazione ferroviaria, 21 décembre 2017.

[28] Schiffer, Zoe, « This girls-only app uses AI to screen a user's gender — what could go wrong? » , *The Verge*, Février 2020.

[29] K Crawford, « Time to regulate AI that interprets human emotions », Nature, Avril 2021.

[30] AI Now Institute, AI Now 2019 Report, Décembre 2019 ; voir également en ce sens Lauren Rhue, « Racial Influence on Automated Perceptions of Emotions », 2018.

[31] Zhimin Chen and David Whitney, "Tracking the Affective State of Unseen Persons", Proceedings of the National Academy of Sciences, 2019.

[32] Jack Gillum and Jeff Kao, « Aggression Detectors: The Unproven, Invasive Surveillance Technology », *ProPublica*, 25 Juin 2019.

[33] Lisa Feldman Barrett, Ralph Adochs, and Stacy Marsella, "Emotional Expressions Reconsidered:Challenges to Inferring Emotion From Human Facial Movements", Psychological Science in the Public Interest 20, no. 1 (Juillet 2019) : 1–68, voir également en ce sens Barrett et al., "Emotional Expressions Reconsidered.".

[34] O'Neil, « Personality tests are failing American workers », *Bloomberg*, Janvier 2018.

[35] Article 8 de la Convention européenne des droits de l'Homme.

[36] Article 7 et article 8 de la Charte des droits fondamentaux de l'Union européenne.

[37] Agence européenne des droits fondamentaux, Conseil de l'Europe et Contrôleur européen de la protection des données, *Manuel sur le droit européen de la protection des données*, juin 2018, p. 19.

[38] CJUE, n° C-212/13, František Ryneš c/ *Úřad pro ochranu osobních údajů*, 2014, point 22.

[39] CNIL, Livre blanc sur les assistants vocaux, p.40.

[40] Règlement UE 2016/679 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 et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

[41] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[42] Il s'agit au titre de l'article 9 du RGPD du traitement de données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, traitement de données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne.

[43] CNIL, « Reconnaissance faciale : pour un débat à la hauteur des enjeux », *op cit*.

[44] Directive 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil ; C'est-à-dire lorsque ces traitements ont lieu aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

[45] CNIL, « Reconnaissance faciale : pour un débat à la hauteur des enjeux », *op cit*.

[46] Discours du Contrôleur européen de la protection des données, EDPS 07.10.2020 « The state of Biometrics », juillet 2020 ; Avis du groupe de travail « article 29 » sur la protection des données n° 3/2012 sur l'évolution des technologies biométriques, Contrôleur européen de la protection des données, *Lignes directrices 3/2019 sur le traitement de données personnelles à travers de dispositifs vidéo*, Janvier 2020 ; Agence espagnole de protection des données, *Rapport sur la reconnaissance faciale*, mai 2020 ; ICO, *Guide to data protection*, novembre 2019.

[47] CNIL, « Reconnaissance faciale : pour un débat à la hauteur des enjeux », *op cit*.

[48] Défenseur des droits, avis n°20-13 du 21 décembre 2020 relatif à la proposition de loi relative à la sécurité globale.

[49] Plus de 175 associations ont cosigné une lettre ouverte appelant à l'interdiction mondiale du recours à la reconnaissance faciale et à la reconnaissance biométrique à distance permettant une surveillance de masse et une surveillance ciblée discriminatoire ; voir en ce sens Access Now, « Ban Biometric Surveillance », 7 juin 2021.

[50] Défenseur des droits, avis 15-25 du 1er décembre 2015 relatif à la sécurité dans les gares face à la menace terroriste : Mission d'information sur la sécurité dans les gares face à la menace terroriste, p.3.

[51] « La reconnaissance faciale s'insinue dans la vie des Russes », L'Express, mars 2021.

[52] Brewster, « Facial Recognition Firms Pitch Covid-19 'Immunity Passports' for America and Britain », Forbes, 2020 ; voir également Ada Lovelace Institute, "International monitor: vaccine passports and COVID status apps", 10 mai 2021, p.58.

[53] Hill, Kashmir, The secretive company that might end privacy as we know it, *New York Times*, janvier 2020 ; voir également Laufer, Meineck, « PimEyes : A Polish company is abolishing our anonymity », *Netzpolitik.org*, Juillet 2020.

[54] European Data Protection Board, « Swedish Dpa : Police unlawfully used facial recognition app », February 2021.

[55] Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta, février 2021.

[56] Voir par exemple F. Reynaud, « Reconnaissance faciale : une enquête demandée à la CNIL sur les pratiques de Clearview », *Le Monde*, mai 2021.

[57] Avis de l'autorité italienne de protection des données sur le système SARI real time, 25 mars 2021.

[58] Proposition de loi nº 4127 d'expérimentation créant un cadre d'analyse scientifique et une consultation citoyenne sur les dispositifs de reconnaissance faciale par l'intelligence artificielle.

[59] Reltien, Philippe, « Reconnaissance faciale : officiellement interdite, elle se met peu à peu en place », Cellule d'investigation de Radio France, septembre 2020.

[60] Au titre du principe de licéité, tout traitement de données à caractère personnel ne peut être légalement mis en œuvre que s'il se fonde sur une « base légale » de traitement (le consentement, l'intérêt légitime, l'obligation légale, la mission d'intérêt public, le contrat, la sauvegarde des intérêts vitaux) ou s'il est nécessaire à l'exécution d'une mission effectuée par une autorité compétente lorsque le traitement a lieu à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.

[61] Au titre du principe de proportionnalité, les données personnelles faisant l'objet d'un traitement doivent être pertinentes et strictement nécessaires à la finalité dudit traitement. Voir également CNIL, « Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position » Octobre 2019 ; CNIL, « Reconnaissance faciale et interdiction commerciale de stade : la CNIL adresse un avertissement à un club sportif », Février 2021.

[62] « Publicly accessible biometric database highlights key failings », *Computer Weekly*, Août 2019.

[63] Voir Lequesne Roth, Caroline, *Les nouvelles technologies de surveillance dans l'espace public : enjeux et perspectives pour la législation européenne*, Agenda Urbain de l'Union européenne, avril 2021 ; Voir également « Major breach found in biometrics system used by banks, UK police and defence firms », *The Guardian*, août 2019.

[64] Défenseur des droits, Avis 20-06 du 17 novembre 2020 relatif au texte adopté par la Commission des lois, sur la proposition de loi relative à la sécurité globale, p.4 ; Voir également CNIL, « Reconnaissance faciale : pour un débat à la hauteur des enjeux », *op cit.* ; Castelluccia, Claude, Le Métayer, Daniel. Analyse des impacts de la reconnaissance faciale – Quelques éléments de méthode. [Rapport de recherche] Inria Grenoble Rhône-Alpes, 2019.

[65] Huszti-Orbán, Krisztina et Ní Aoláin, Fionnuala, L'utilisation des données biométriques pour identifier les terroristes: meilleure pratique ou pratique risquée ?, Human Rights Center, University of Minnesota, juillet 2020.

[66] Un faux positif correspond à une situation où l'algorithme pense à tort qu'il n'y a pas de correspondance tandis qu'un faux négatif correspond à la situation où l'algorithme pense à tort qu'il y a correspondance.

[67] Hill, Kashmir, « Wrongfully accused by an algorithm », *New York Times*, août 2020.

[68] Erreurs en fonction du genre : Buolamwini, Joy et Gebru, Timnit, « Gender Shades, Intersectional Accuracy Disparities in Commercial Gender Classification », Proceedings of the 1st Conference on Fairness, Accountability and Transparency, 2018 ; erreurs en fonction du sexe, de l'âge, de la couleur de peau : Grother, P., Ngan, M., and Hanaoka, *Ongoing Face Recognition Vendor Test (FRVT). Part 1: Verification*, avril 2019 ; erreurs en fonction de l'âge : Raji, Inioluwa Deborah, Gebru, Timnit, Mitchell, Margaret, Buolamwini, Joy, Lee, Joonseok et Denton, Emily. 2020. « Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing ». In *Proceedings of the 2020 AAAI/ACM Conference on AI, Ethics, and Society* (AIES '20), February 7–8, 2020, février 2020, Agence des droits fondamentaux de l'Union européenne, *Technologie de reconnaissance faciale: considérations relatives aux droits fondamentaux dans le maintien de l'ordre*, novembre 2019.

[69] Lorsque les algorithmes sont entraînés très majoritairement sur des photos d'hommes blancs, on observe des mauvaises performances lors de leur utilisation sur d'autres types de profils ; voir Buolamwini, Joy et Gebru, Timnit, « Gender Shades, Intersectional Accuracy Disparities in Commercial Gender Classification », Proceedings of the 1st Conference on Fairness, Accountability and Transparency, 2018

[70] Déclaration du Défenseur des droits, « Algorithmes, prévenir l'automatisation des discriminations », mai 2020.

[71] *Op. Cit*. Note n°65.

[72] Agence des droits fondamentaux de l'Union européenne, Technologie de reconnaissance faciale: considérations relatives aux droits fondamentaux dans le maintien de l'ordre, novembre 2019, p. 9.

[73] Comme c'est le cas du système Parafe. Voir en ce sens Grother, P., Ngan, M., and Hanaoka, *Ongoing Face Recognition Vendor Test (FRVT). Part 1: Verification*, avril 2019.

[74] L'authentification en ligne certifiée sur mobile (ALICEM) est un dispositif utilisant la reconnaissance faciale actuellement expérimenté en France. Dans sa décision Alicem du 4 novembre 2020, le Conseil d'Etat a considéré que « dès lors que les usagers qui ne consentiraient pas au traitement prévu dans le cadre de la création d'un compte Alicem peuvent accéder en ligne [via le service FranceConnect], grâce à un identifiant unique, à l'ensemble des téléservices proposés, ils ne sauraient être regardés comme subissant un préjudice au sens du règlement général sur la protection des données précité ». En l'espèce, le Conseil d'Etat a ainsi considéré que le portail FranceConnect (dispositif permettant aux internautes de s'identifier sur un service en ligne par l'intermédiaire d'un compte existant (ameli.fr, impots.gouv.fr entre autres) constituait une voie alternative suffisante à l'utilisation du dispositif Alicem pour vérifier l'identité des internautes.

[75] Voir par exemple : Lomas, « Uber under pressure over facial recognition checks for drivers », *TechCrunch*, Mars 2021.

[76] Cela s'explique par la qualité de la source de l'image, qu'il s'agisse d'une photo ou d'une vidéo. Dans un environnement non contrôlé les paramètres d'éclairage, d'exposition, etc. changent et peuvent dégrader la précision du dispositif.

[77] Voir *Op. Cit*. notes 66 & 67.

[78] FRA European Union Agency for Fundamental Rights, Facial recognition technology : fundamental rights considerations in the context of law enforcement.

[79] Hill, Kashmir, « Another arrest and jail time due to a bad facial recognition match », *New York Times*, Décembre 2020.

[80] Fussey, Pete et Murray, Daragh, Independent Report on the London Metropolitain Police Service's Trial of Facial Recognition Technology, The Human Rights, Big Data and Technology Project, juillet 2019.

[81] Court of appeal, *R (Bridges) v Chief Constable of South Wales Police*, 2019, EWHC 2341 (Admin).

[82] Défenseur des droits, Enquête sur l'accès aux droits. Vol.1 : Rapports police / population. L'étude sur l'accès aux droits (vol. 1) réalisée sur un échantillon représentatif de plus de 5000 personnes a été publiée en 2017.

[83] C'est-à-dire de constatation des infractions par vidéo suivie de l'envoi, par exemple, d'une contravention par voie postale.

[84] Défenseur des droits, Décision 2020-102 du 12 mai 2020 relative à des observations devant le tribunal judiciaire de X dans le cadre d'une procédure en responsabilité de l'Etat pour contrôles d'identité discriminatoires, p.9.

[85] Voir en ce sens Rapport Défenseur des droits, « La défaillance du forfait de post-stationnement : rétablir les droits des usagers », 13 janvier 2020.

[86] Commission européenne, Proposal for a Regulation laying down harmonised rules on artificial intelligence, avril 2021, Art. 5 paragraphe 1 point d (iii).

[87] Agence des droits fondamentaux de l'Union européenne (FRA), « Être noir dans l'UE : Deuxième enquête de l'Union européenne sur les minorités et la discrimination : Résumé », *op.cit*.

[88] Commission Européenne, « Intelligent Portable Border Control System », Horizon 2020 ; voir également en ce sens « IBorderCtrl : Intelligent Portable Contyrol System Project » .

[89] iBorderCtrl demande tout d'abord aux voyageurs de télécharger des photos de leur passeport, de leur visa et d'autres éléments qui sont ensuite transmis à l'intelligence artificielle qui les attend ensuite au poste frontière. Cette IA pose alors des questions via un haut-parleur et analyse les réponses humaines grâce à une webcam afin de détecter les micro-expressions présentes sur les visages des voyageurs. À la suite de cet interrogatoire par la machine, un jeton est délivré au voyageur : s'il est soupçonné par le système iBorderCtrl d'avoir menti, le jeton le mène à une file d'attente où des gardes-frontière vont récupérer des données biométriques (empreintes digitales et des veines de la main, reconnaissance faciale) pour prolonger le contrôle ; si la machine n'a pas détecté de mensonge, le jeton donné au voyageur par l'IA le mène à une file à "bas risque", avec moins de contrôles.

[90] Voir en ce sens : E. Chelloudakis, « Greece : Clarifications sought on human rights impacts of iBorderCtrl », *EDRi*, Novembre 2018. Le système était en 2018 crédité d'un taux de réussite autour de 75%, ce qui laisse donc un quart des voyageurs pouvant être soupçonnés de mentir alors que ce n'est pas le cas. Un député européen a par ailleurs déposé une action en justice afin de faire toute la lumière sur les origines de cette expérimentation peu éthique, et visant à obtenir des réponses concernant notamment le profil des individus victimes de faux positifs afin d'identifier de potentielles discriminations causées par ce système. Voir P. Breyer, « EU-funded technology violates fundamental rights », *about :intel*, 22 avril 2021 ; voir également en ce sens Parlement Européen, Question for written answer E-000152/2020 to the Commission, Rule 138, Patrick Breyer (Verts/ALE), Janvier 2020.

[91] Sur le modèle de l'américain HireVue, l'entreprise hexagonale Itwapp par exemple propose de réaliser des entretiens vidéo différés agrémentés d'IA qui va trier les candidats d'après les données suggérées par leur expressions faciales et orales. Par l'analyse du langage corporel et oral, l'IA analyserait l'ouverture (curiosité), son caractère consciencieux (contrôle, discipline…), l'extraversion, l'agréabilité et la négativité du candidat. La machine classe les éléments de langage du candidat, la richesse de son vocabulaire, l'intonation, la modulation de sa voix, la longueur de ses phrases, révélatrice de sa capacité à synthétiser, son débit de parole, etc. et ces données sont corrélées avec le test Big Five, test de personnalité classique. La start-up affirme ne pas recourir à l'analyse faciale, la technologie étant loin d'être au point. Elle propose, pour l'instant, à ses clients de retranscrire l'intégralité du discours du candidat pour l'évaluer selon cinq critères : prosodie (accentuation, intonation), fluidité du propos, habileté verbale, débit de parole et contenu verbal. Il faut moins de trois minutes à la machine pour analyser ces critères et proposer une classification notée entre les candidats ayant répondu à la même offre.

[92] A. Engler, « For some employment algorithms, disability discrimination by default », Brookings, Octobre 2019.

[93] Krassovsky, Julie, « Recrutement : quelles sont les limites de l'intelligence artificielle ? », *Capital*, Avril 2020.

[94] Knight, Will, « Job screening service halts facial analysis of applicants », *Wired*, janvier 2021.

[95] Ces techniques sont censées permettre d'évaluer les futures performances professionnelles du candidat, sa capacité à manager ou encore certaines qualités recherchées. L'efficacité consiste donc ici à repérer la candidate ou le candidat qui sera effectivement performant une fois titulaire de l'emploi.

[96] Code du travail, art. L1221-6 section 2.

[97] Voir en ce sens A compétence égale, Charte « Algorithmes, intelligence artificielle et recrutement ».

[98] Discours du Contrôleur européen de la protection des données, EDPS 07.10.2020 « The state of Biometrics », juillet 2020 ; voir également ACLU, « Does Surveillance Affect Us Even When We Can't Confirm We're Being Watched? Lessons From Behind the Iron Curtain », 2012.

[99] International Justice and Public Safety Network (2011), Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field, 30 Juin 2011.

[100] Human Rights Council (2019), Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/41/35.

[101] CNIL, Délibération de la formation restreinte n°SAN-2021-003 du 12 janvier 2021 concernant le ministère de l'intérieur.

[102] Décision n°2021-817 DC du 20 mai 2021.

[103] Défenseur des droits, Avis 20-05 du 3 novembre 2020 relatif à la proposition de loi relative à la sécurité globale.

[104] Rapport OL FRA 4/2020 Mandats de la Rapporteuse spéciale sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste; de la Rapporteuse spéciale sur la promotion et la protection du droit à la liberté d'opinion et d'expression; et du Rapporteur spécial sur le droit de réunion pacifique et la liberté d'association, 12 Novembre 2020.

[105] Loi n°2021-646 du 25 mai 2021, art. 47 (V).

[106] Rapport de la Rapporteuse spéciale sur les formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée, 10 Novembre 2020.

[107] CNIL, Délibération 00-015 du 21 mars 2000.

[108] Ancien article 25 de la loi du 6 janvier 1978 dite Informatique et Libertés.

[109] EDPB, « Facial recognition in school renders Sweden's first GDPR fine », Août 2019.

[110] CNIL, «Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position », Octobre 2019.

[111] RGPD, Considérants 38 et 58.

[112] FRA (2018), *The revised Visa Information System and its fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights*, FRA Opinion 2/2018 [VIS], Vienna, 30 Août 2018, pp. 67-69.

[113] Déclaration du Défenseur des droits, « Algorithmes, prévenir l'automatisation des discriminations », mai 2020.

[114] The Hamburg Commissioner for Data Protection and Freedom of Information, « Administrative order on Information issued against Clearview AI -Transparent answers on Data Protection required ! », Août 2020 ; CNIL, « Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position », Octobre 2019 ; CNIL, « Surveillance des examens en ligne : les rappels et conseils de la CNIL », 20 mai 2020.

[115] Parlement Européen, Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application, Mars 2021.

[116] Tisné M., « Collective data right scan stop big tech from obliterating privacy » *MIT Technology Review*, 25 Mai 2021, voir également également Tisné, « The data delusion : protecting individual data isn't enough when the harm is collective ».

[117] LOI n° 2008-496 du 27 mai 2008 portant diverses dispositions d'adaptation au droit communautaire dans le domaine de la lutte contre les discriminations, Art. 1.

[118] Xenidis R., Gerards J., Algorithmic discrimination in Europe, Challenges and opportunities for gender equality and non-discrimination law, Publications Office of the EU, Mars 2021, p.49.

[119] Huszti-Orbán & Ní Aoláin, L'utilisation des données biométriques pour identifier les terroristes : meilleure pratique ou pratique risquée ? - Résumé des conclusions et recommandations, Human Rights Center University of Minnesota (2020).

[120] CNIL, « Reconnaissance faciale : pour un débat à la hauteur des enjeux », novembre 2019 ; voir également CNIL, « Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position », Octobre 2019 ; CNIL, « La CNIL appelle à la vigilance sur l'utilisation des caméras dites « intelligentes » et des caméras thermiques », Juin 2020 ; CNIL, « Caméras dites « intelligentes » et caméras thermiques : les points de vigilance de la CNIL et les règles à respecter », Juin 2020.

[121] Commission européenne, Proposal for a Regulation laying down harmonised rules on artificial intelligence, avril 2021, p. 19.

[122] Conseil de l'Europe, Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Convention 108, Lignes directrices sur la reconnaissance faciale, Janvier 2021.

[123] CEPD-EDPS, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 juin 2021, p.2.

[124] Conseil d'État Décision n° 439360, paragraphe 13.

[125] Conseil de l'Europe, Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne, Convention 108, Lignes directrices sur la reconnaissance faciale, Janvier 2021, p.3.

[126] Cas par exemple d'un policier qui souhaiterait retrouver une personne en particulier sans motif valable.

[127] Voir en ce sens, European Data Protection Supervisor, « Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary », Avril 2021.

[128] CEPD-EDPS, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 juin 2021, p.2.

[129] LOI n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés, Art. 47.

[130] Voir Lequesne Roth, Caroline, *Les nouvelles technologies de surveillance dans l'espace public : enjeux et perspectives pour la législation européenne*, Agenda Urbain de l'Union européenne, avril 2021.

[131] Défenseur des droits, Rapport, Dématérialisation et inégalités d'accès aux services publics, 2019, p.29.

[132] Conseil de l'Europe, Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne, Convention 108, Lignes directrices sur la reconnaissance faciale, Janvier 2021, p.3.

[133] *Op. Cit.* Note 72.

[134] Déclaration du Défenseur des droits, « Algorithmes, prévenir l'automatisation des discriminations », mai 2020.

[135] Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique.

[136] Ce seuil de 9 millions est fixé à l'article 1er de l'arrêté du 5 juin 2020. Voir en ce sens, Arrêté du 5 juin 2020 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique.

[137] La proposition prévoit entre autres l'obligation de prévoir des mécanismes adéquats d'évaluation et d'atténuation des risques, de garantir une haute qualité des données mobilisées par le système afin de minimiser les risques et les situations discriminatoires, d'assurer la traçabilité de toute utilisation du dispositif, de fournir une documentation détaillée rassemblant toutes les informations nécessaires sur le système et son objectif afin que les autorités puissent évaluer sa conformité, d'informer l'utilisateur en des termes clairs et compréhensibles sur le fonctionnement du dispositif, de prévoir des mesures de supervision humaine appropriées pour minimiser les risques, de garantir un haut niveau de fiabilité, de sécurité et de précision du système ; voir en ce sens T. Christakis, « Facial recognition in the draft European AI regulation : final report on the high-level workshop held on April 26, 2021 », 27 Mai 2021.

[138] Commission européenne, Proposal for a Regulation laying down harmonised rules on artificial intelligence, avril 2021, Art. 43

[139] Déclaration du Défenseur des droits, « Algorithmes, prévenir l'automatisation des discriminations », mai 2020.

[140] CNIL, « Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données (AIPD) », 22 octobre 2019.

[141] Commission européenne, Proposal for a Regulation laying down harmonised rules on artificial intelligence, avril 2021, Art. 43.

Défenseur des droits

TSA 90716 - 75334 Paris Cedex 07

Tél. : 09 69 39 00 00

defenseurdesdroits.fr

Toutes nos actualités :

defenseurdesdroits.fr

Défenseurdesdroits

RÉPUBLIQUE FRANÇAISE