LES NOTES SCIENTIFIQUES DE L'OFFICE
OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES

Note n° 14 — La reconnaissance faciale — Juillet 2019

123fr©AndriyPopov

Résumé

- *Les progrès liés au développement de l'intelligence artificielle, en particulier l'apprentissage profond (deep learning) ont permis aux outils de reconnaissance faciale de devenir beaucoup plus performants. Ils semblent aujourd'hui à la portée de tous : applications pour smartphone, paiement automatique, contrôle d'identité aux frontières…*
- *Souvent méconnue des citoyens, une large économie se développe autour de l'exploitation des données et s'accompagne de nombreuses craintes quant aux applications qui pourraient porter atteinte aux libertés fondamentales.*
- *Il semble nécessaire d'élaborer un cadre législatif d'expérimentation afin de tester ces dispositifs en conditions réelles et garantir notre souveraineté pour ne pas être dépendant des solutions mises au point par les géants du numérique, puis de définir un cadre de régulation au plus près des usages.*

M. Didier Baichère, Député, Vice-Président

Contexte technologique

La reconnaissance faciale est apparue depuis peu dans le débat public, en particulier depuis l'expérimentation récente menée par la mairie de Nice, ou l'interdiction par la ville de San Francisco de l'utilisation par ses services de tels dispositifs. Il a donc paru nécessaire à l'Office d'étudier les enjeux technologiques, éthiques, juridiques et sociologiques relatifs à cette technologie.

La vision par ordinateur est un domaine de l'intelligence artificielle[1] (IA) qui analyse des images de façon automatique. La reconnaissance faciale est une branche de la vision par ordinateur qui s'intéresse à l'analyse biométrique des visages présents sur une image. Ces technologies ont connu un fort gain en performance ces dernières années grâce aux progrès des algorithmes liés à l'utilisation de l'apprentissage profond (*deep learning*) et des technologies de capteurs.

Le processus peut être décrit schématiquement de la façon suivante : l'algorithme extrait d'une photo un gabarit, sorte de signature propre à chaque visage, puis il compare les gabarits issus d'autres images afin de déterminer si elles correspondent à une même personne. Il est important de rappeler que les dispositifs de reconnaissance faciale ne donnent pas de résultat absolu ; les résultats sont exprimés en un pourcentage de correspondance. Il faut donc faire le choix du seuil[2] de correspondance à partir duquel on décide que deux gabarits proviennent certainement de la même personne[3].

La reconnaissance faciale ne doit pas être confondue avec l'analyse faciale ou la reconnaissance d'émotion, qui visent à déterminer certaines caractéristiques (âge, sexe, origine ethnique, émotions…) des personnes présentes sur une image. Ces deux derniers domaines ne font pas intervenir de données biométriques et sont donc moins sensibles que la reconnaissance faciale *stricto sensu*. De nombreuses applications commerciales utilisant la reconnaissance faciale, l'analyse faciale et la reconnaissance d'émotion se développent : marketing ciblé, déverrouillage d'appareils électroniques[4], applications bancaires[5], mais aussi aide au diagnostic[6] ou détection de stress chez des personnes vulnérables[7]. L'automatisation de processus fastidieux et chronophages reste cependant la principale application de la reconnaissance faciale[8].

Par exemple, l'analyse en temps réel et en temps différé des images de vidéoprotection peut permettre aux forces de l'ordre de détecter plus rapidement les scènes d'intérêt. Ainsi ces dispositifs connaissent des applications potentielles en matière de sécurité intérieure et de police[9]. Actuellement en France, leur utilisation par les forces de police et de gendarmerie est limitée : à la comparaison d'images obtenues lors d'une enquête avec le traitement des antécédents judiciaires (TAJ), seul fichier de police judiciaire permettant de recourir à la reconnaissance faciale[10] ; au

Assemblée nationale - 101 rue de l'Université - 75355 Paris 07 SP – Tél : 01 40 63 26 81 – Mél : secretariat-opecst@assemblee-nationale.fr
Sénat - 15 rue de Vaugirard - 75291 Paris Cedex 06 – Tél : 01 42 34 25 58 – Mél : opecst-secretariat@senat.fr

dispositif Parafe[11] lors du passage de frontières extérieures ; et au dispositif d'identification numérique ALICEM[12]. Le comité d'organisation des Jeux Olympiques de 2020, qui auront lieu à Tokyo, prévoit d'utiliser des portiques dotés de dispositifs de reconnaissance faciale afin de contrôler les accès réservés aux athlètes, aux membres du personnel et aux journalistes[13].

Enfin, pour être reconnue, une personne doit avoir été « enrôlée », *c'est-à-dire* incluse dans la base à laquelle les images sont comparées. La question des données sur lesquelles est réalisé le traitement de reconnaissance faciale est donc primordiale.

Authentification ou identification ?

Il est important de distinguer deux types d'utilisations des dispositifs de reconnaissance faciale :

– On parle d'authentification lorsqu'il s'agit de déterminer si une personne correspond à ce qu'elle prétend être. Il s'agit donc de comparer un gabarit extrait d'une photo prise lors du processus à un gabarit préenregistré.

➢ Exemples : dispositifs Parafe (voir *infra*) ou de déverrouillage de téléphone

– On parle d'identification lorsque l'on souhaite retrouver l'identité d'une personne à partir d'une image en la comparant avec plusieurs autres réunies au sein d'une base d'images précédemment constituée.

➢ Exemple : vidéoprotection intelligente

Une technologie encore imparfaite

Malgré les progrès réalisés au cours des dernières années les dispositifs de reconnaissance faciale ne sont pas encore parfaitement efficaces. Les conditions d'utilisation ont un véritable impact sur le taux de succès de ces dispositifs. Dans des conditions contrôlées (éclairage, angle de prise de vue, immobilité), comme cela est le cas par exemple pour le dispositif Parafe, le taux de fiabilité peut atteindre des valeurs supérieures à 99,5 %. La situation est toute autre dans des environnements non contrôlés. Le *National Institute of Standards and Technology* (NIST), agence américaine chargée de mener des tests sur les dispositifs de reconnaissance faciale, a publié un rapport en novembre 2018 sur la performance des algorithmes d'identification[14] qui atteste des progrès réalisés tout en relevant les effets négatifs de différents facteurs, comme la qualité des images utilisées ou encore le vieillissement des individus, sur le taux de réussite de ces algorithmes. Des enquêtes[15] ont montré de plus qu'il était possible de tromper ces algorithmes en utilisant par exemple des masques fabriqués à l'aide d'imprimantes 3D[16]. De nombreuses expérimentations menées à l'étranger ont souligné les progrès qui pouvaient encore être faits[17].

Des biais qui persistent

Plusieurs études ont fait état d'écarts de performance des algorithmes de reconnaissance faciale entre différentes catégories de population. Joy Buolamwini, chercheuse au *Massachusetts Institute of Technology*, a établi[18] que ceux-ci tendent à moins bien reconnaître les femmes noires que les hommes blancs. De la même façon, le NIST, dans un rapport publié en avril 2019[19], a souligné que l'ensemble des algorithmes étaient systématiquement moins performants pour reconnaître une femme que pour reconnaître un homme. Cela provient principalement du manque de diversité des bases d'images utilisées pour entraîner les algorithmes. Cet enjeu revêt une importance particulière et doit être étudié. Plusieurs acteurs ont exposé, lors des auditions menées pour l'élaboration de cette note, leurs efforts pour accroître la diversité de leurs bases. La situation semble s'améliorer, comme l'a montré Joy Buolamwini dans une autre étude[20] .

Un cadre juridique existant…

Un certain nombre de dispositions légales nationales et européennes encadrent dès à présent l'utilisation des dispositifs de reconnaissance faciale. Le cadre d'emploi dépend principalement de l'usage fait de ces dispositifs :

- Utilisation par l'État dans le cadre de ses prérogatives de puissance publique

En France, les traitements de données biométriques pour le compte de l'État dans le cadre de ses prérogatives de puissance publique sont encadrés par les articles 31 et 32 de la loi « informatique et libertés »[21] et par l'article 10 de la directive européenne n° 2016/680[22] . Ces dispositions viennent limiter le champ d'application de ces traitements[23] et imposent pour leur mise en œuvre un décret en Conseil d'État pris après l'avis de la CNIL[24]. L'utilisation de la reconnaissance faciale couplée à un système de vidéoprotection ou à d'autres fichiers de police judiciaire doit s'inscrire dans ce cadre juridique.

- Utilisations dans un autre cadre

Dans l'Union européenne, depuis le 25 mai 2018, la mise en place de traitements mobilisant des données personnelles est encadrée par le règlement général sur la protection des données (RGPD)[25]. L'utilisation de dispositifs de reconnaissance faciale, faisant intervenir des données biométriques, particulièrement sensibles parce qu'elles permettent d'identifier de façon unique un individu, doit donc se conformer aux dispositions introduites par ce règlement. En particulier, le responsable d'un traitement doit effectuer une analyse d'impact relative à la protection des données[26] et la transmettre à la CNIL, pour consultation

préalable, en cas de détection de risques résiduels élevés. Dès lors, la CNIL n'est plus systématiquement informée de la mise en place de ces dispositifs et n'a plus à donner son accord *a priori*. En contrepartie, ce nouveau système vise à la responsabilisation[27] de l'auteur du traitement et de son sous-traitant, qui est considéré comme coresponsable. Pour ce type d'utilisation, le consentement[28] est une des bases légales possibles[29], ce qui pose la question des modalités de recueil de ce consentement (affichage à l'entrée d'un magasin…). Le RGPD permet de déroger à certaines règles lorsque le traitement est effectué à des fins de recherche scientifique.

… mais incomplet

L'expérimentation menée à Nice[30] a mis au jour la nécessité de compléter le cadre juridique actuel.

Expérimentation menée à Nice lors de la 135e édition du carnaval (février 2019)

La mairie de Nice a mené pendant trois jours la première expérimentation en conditions réelles d'un dispositif de reconnaissance faciale en France. Plusieurs scénarios ont été testés au cours de cette expérimentation (recherche d'enfants perdus et de personnes vulnérables, fluidification des points d'accès, contrôle d'accès restreints…) sur des personnes consentantes.

Cette expérimentation se plaçait dans un cadre régi par le RGPD, le fondement légal utilisé étant la recherche scientifique et non pas la sécurité. Même si la CNIL n'a pas eu à fournir d'autorisation préalable, un travail commun de la CNIL et de la mairie de Nice a cependant été mené peu de temps avant le carnaval, afin d'assurer le respect des dispositions du RGPD.

Les représentants d'entreprises, d'organismes de régulation, d'acteurs publics ont exprimé leur souhait de voir élaborer des dispositions légales autorisant la mise en place d'expérimentations à grande échelle de dispositifs de reconnaissance faciale afin de tester en conditions réelles les avantages et les limites de ces technologies, tant techniquement que sociologiquement, et ainsi d'être en capacité de les maîtriser, mais également de proposer un cadre légal au plus près des usages et respectueux des libertés fondamentales.

Le développement des dispositifs de reconnaissance faciale et leur diffusion hors d'Europe sont inéluctables, tant les usages se multiplient et tant le nombre d'acteurs qui investissent dans ces technologies, au premier rang desquels les géants du numérique GAFA (Google, Amazon Facebook, Apple et Microsoft) et BATX (Baidu, Alibaba, Tencent et Xiaomi), croît. La France doit donc, afin de préserver sa souveraineté, soutenir la recherche et l'innovation[31] sur ces dispositifs dans le cadre de la filière IA.

Des technologies qui imposent la tenue d'un débat de société

Les collectivités locales sont déjà exposées à ces sujets au travers du déploiement plus ou moins important de caméras de vidéoprotection dans les agglomérations. Comme en témoignent les échanges avec l'Association des maires de France (AMF), les élus sont sensibilisés aux conséquences de la « *safe city* »[32] sur les libertés individuelles ; l'acceptation par les citoyens est un point clé du potentiel déploiement de solutions de reconnaissance faciale.

La CNIL a récemment appelé à la tenue d'un débat démocratique sur ces questions[33]. Ce débat doit permettre aux différents acteurs de s'exprimer sur la question de l'autorisation, de l'encadrement ou de l'interdiction de certains usages, qui ne pourra être traitée de façon pérenne qu'après l'expérimentation en condition réelle de ces dispositifs.

Des craintes sont régulièrement exprimées[34] sur les risques que ferait peser la diffusion des dispositifs de reconnaissance faciale sur nos libertés fondamentales (liberté de circuler anonymement, liberté de manifester…) et sur la possibilité de voir se développer une surveillance généralisée de la population. L'exemple de la Chine[35] est le plus marquant, avec l'intégration des éléments recueillis à l'aide de la reconnaissance faciale dans le système de crédit social[36], ou encore le contrôle des populations Ouïghours dans le Xinjiang[37]. Ces craintes doivent être prises en compte et la diffusion de ces dispositifs doit pouvoir se faire sans porter atteinte aux droits fondamentaux. Pour Laurent Mucchielli, sociologue au CNRS : « La technologie n'est ni bonne ni mauvaise en soi. Tout dépend des usages que nous décidons d'en faire et des arbitrages financiers qui sont faits derrière nos choix. »[38]. Selon Jean-Gabriel Ganascia, président du comité d'éthique du CNRS, ces craintes pourraient être levées en distinguant les usages et en autorisant seulement ceux ne présentant pas de risque.

Le Conseil national du numérique et le Centre pour la quatrième révolution industrielle (C4IR) du Forum économique mondial lancent un projet pilote d'une durée de 12 mois pour alimenter le débat démocratique sur l'encadrement des technologies de reconnaissance faciale, au niveau national, européen et mondial. Ce projet vise à co-construire un cadre de régulation de la reconnaissance faciale qui garantisse la protection des libertés individuelles[39].

Les géants du numérique ont fait part publiquement de leur prise en considération des enjeux sociétaux soulevés par ces dispositifs. Microsoft, par la voix de son président Brad Smith, a demandé aux législateurs de réguler ce domaine[40] et mis en place des principes

qui structurent sa stratégie en matière de reconnaissance faciale[41]. Sundar Pichai, PDG de Google, a fait de même en publiant les sept principes de son entreprise sur l'IA[42]. Qwant a fait le choix d'intégrer aux dispositifs de reconnaissance faciale qu'il met en place des outils permettant par exemple de flouter l'ensemble des visages[43]. Amazon adopte une démarche moins volontariste et ne se considère pas responsable des utilisations pouvant être faites de ses outils[44].

La France pourrait se positionner en exemple sur ces questions. Elle bénéficie en effet de chercheurs de très grande qualité et dispose d'entreprises parmi les plus performantes internationalement – comme IDEMIA, leader mondial de la biométrie, ou Gemalto, leader mondial de la sécurité numérique – et de start-ups dynamiques comme XXII Group.

Ces technologies pourraient également connaître un développement important dans le domaine militaire[45]. Au ministère des armées, l'agence de l'innovation de la défense de la direction générale de l'armement (DGA) a été créée le 1er septembre 2018 ; la ministre Florence Parly a également annoncé la création d'un « comité d'éthique ministériel sur les sujets de défense ». Ces deux organismes ont pour objet de mener une véritable réflexion éthique sur les applications de ces technologies dans le secteur de la défense.

Un sujet débattu dans de nombreux pays

L'implantation des dispositifs de vidéoprotection au Royaume-Uni en a fait un terrain propice à la diffusion rapide des dispositifs de reconnaissance faciale[46]. Le *Metropolitan Police Service* a mené de nombreuses expérimentations[47] qui se sont révélées être pour la plupart en deçà de leurs attentes. Des dispositifs commerciaux sont également déjà présents, par exemple le *Children's Charity Plan UK*, qui cible sa campagne de publicité dans le bus en fonction du sexe du passager. Le cadre d'utilisation de ces dispositifs est actuellement en pleine évolution. En juin 2018, le ministère de l'intérieur a publié une stratégie sur les technologies biométriques[48] visant à compléter les dispositions existantes[49].

Aux Pays-Bas, les forces de l'ordre étudient, en partenariat avec le *Netherlands Forensic Institute*, la possibilité d'utiliser la reconnaissance faciale lors d'enquêtes pénales ou pour lutter contre le terrorisme, en munissant des patrouilles de caméras corporelles connectées à une base de données. Dans un cadre commercial, l'enseigne de grandes surfaces alimentaires *Jumbo Ten Brink Food* a récemment installé des dispositifs de reconnaissance faciale pour lutter contre le vol à l'étalage.

La reconnaissance faciale est actuellement l'objet d'un débat important aux États-Unis. Regroupant de nombreuses entreprises en pointe dans ce domaine, la reconnaissance faciale est très utilisée par les forces de l'ordre. Cependant, la situation est variable d'un État à l'autre, aucune disposition fédérale ne venant encadrer ces dispositifs. Des demandes de régulation se font depuis peu entendre : plusieurs villes, à l'instar de San Francisco, ont récemment annoncé interdire l'utilisation de cette technologie par leurs services et un projet de loi bipartisan[50] a été déposé en ce sens.

Conclusions et recommandations

Les dispositifs de reconnaissance faciale sont déjà présents dans notre quotidien, deviennent de plus en plus performants et leur généralisation semble inéluctable. Cette diffusion soulève des enjeux sociétaux, juridiques et éthiques. Afin de permettre le développement de ces technologies tout en garantissant le respect des droits fondamentaux des individus, les recommandations suivantes peuvent être formulées :

– Élaborer rapidement un cadre législatif permettant d'accompagner les expérimentations[51] au profit de l'écosystème industriel et universitaire français. Il conviendrait que la CNIL soit dotée d'un rôle d'accompagnement de l'innovation et d'incitation au « *privacy by design* »[52] dans le domaine de la reconnaissance faciale et plus généralement pour l'ensemble des nouvelles technologies utilisant des données personnelles, sur le modèle de ce que fait l'Autorité de régulation des communications électroniques et des postes (ARCEP)[53], tout en assurant le respect des libertés fondamentales, la souveraineté de la France et le développement d'une IA éthique ;

– Constituer, comme le proposait le rapport de Cédric Villani sur l'intelligence artificielle[54], au sein d'un organisme choisi, un corps d'experts pluridisciplinaires dotés des compétences requises pour auditer les dispositifs de reconnaissance faciale afin de garantir l'efficacité des technologies mises sur le marché en fonction des catégories de besoins, ainsi que l'absence de biais ;

– Réaffirmer la responsabilité de l'ensemble des acteurs : concepteur, intégrateur, responsable du traitement. Il ne serait pas envisageable que certains acteurs, parmi lesquels des géants du numérique, puissent s'exonérer de toute responsabilité éthique ;

– Garantir une validation humaine pour les utilisations les plus sensibles (procédure judiciaire…).

– Mener des études sur l'acceptabilité de ces technologies par les différentes catégories de la population ;

– Améliorer la formation à l'économie de la donnée pour permettre aux décisions d'être prises de façon éclairée et en s'affranchissant des mythes auxquels renvoient ces technologies

Site Internet de l'OPECST :
http://www.assemblee-nationale.fr/commissions/opecst-index.asp
http://www.senat.fr/opecst/

Personnes auditionnées

Mme Véronique Borré, directrice adjointe de cabinet du maire de Nice, M. Gildas Berthier, chef de service de police municipale, Mme Sandra Bertin, directrice de police municipale, MM. Grégory Pezet, chef du centre de supervision urbain, Franck Curinga, direction des systèmes d'information et de la *Smart city,* Jean-François Ona, chargé de mission « sécurité » et Stephan Louppe, directeur des opérations de Confidentia, lors d'une mission à Nice le 14 juin 2019 ;

M. Jean-Christophe Fondeur, directeur de la R&D, membre du comité exécutif, M. Pascal Fallet, senior vice-président Europe pour les activités « Identité et Sécurité publique », et Mme Céline Stierlé, directrice des relations presse et des affaires publiques pour IDEMIA ;

Mmes Florence Fourets, directrice chargée de projets régaliens, Émilie Seruga-Cau, cheffe du service des affaires régaliennes et des collectivités territoriales et Tiphaine Havel, conseillère pour les questions institutionnelles et parlementaires au sein de la Commission nationale de l'informatique et des libertés (CNIL) ;

MM. Julien Groues, directeur, Stéphane Hadinger, directeur de l'Innovation et Lionel Benatia, directeur des affaires publiques d'Amazon Web Service (AWS) France ;

Mme Nathalie Koenders, première adjointe au maire de Dijon, présidente de la commission sécurité, M. Juan Companie, chargé de mission « sécurité » auprès du directeur général et Mme Charlotte de Fontaines, chargée des relations avec le Parlement de l'Association des maires de France (AMF) ;

MM. Éric Léandri, co-fondateur et président-directeur général, Christophe Sevran, directeur scientifique, Sébastien Ménard, conseiller spécial du comité exécutif, Maxime Portaz, chercheur chez Qwant ;

Mme Aurélie Misséré, animateur d'ensemble des projets en IA, MM. Florent Montreuil, expert IA et reconnaissance automatique multi-capteur et Mattis Paulin, architecte projet à la direction générale de l'armement (DGA) du ministère des armées ;

MM. Cédric O, secrétaire d'État auprès du Premier ministre, chargé du numérique et Bertrand Pailhès, coordonnateur national pour la stratégie d'intelligence artificielle ;

M. Bernard Ourghanlian, directeur technique et sécurité et Mme Camille Vaziaga, responsable des affaires publiques chez Microsoft France ;

M. Ludovic Péran, responsable des politiques publiques et des affaires gouvernementales chez Google France ;

M. Renaud Vedel, préfet, coordonnateur au sein du ministère de l'intérieur en matière d'intelligence artificielle, général Bruno Poirier-Coutansais, directeur du service des technologies de la sécurité intérieur (STSI^2), et M. Vincent Niebel, directeur des systèmes d'information et de communication au sein du ministère de l'intérieur.

Experts consultés

Mme Virginie Tournay, membre du conseil scientifique de l'Office, directrice de recherche au CNRS, centre de recherches politiques de Sciences Po (CEVIPOF) ;
M. Serge Abiteboul, directeur de recherche à l'INRIA et à l'ENS, membre de l'Académie des sciences, membre du collège de l'Autorité de régulation des communications électroniques et des postes (ARCEP) ;
M. François Brémond, directeur de recherche à l'INRIA, groupe STARS ;
M. Jean Cattan, conseiller du président de l'ARCEP ;
M. James Crowley, directeur de recherche à l'INRIA, groupe Pervasive Interaction ;
M. Mohamed Daoudi, professeur d'informatique à l'IMT Lille Douai, laboratoire CRIStAL ;
M. Jean-Luc Dugelay, professeur d'informatique à EURECOM ;
M. Jacques Ehrmann, directeur exécutif « patrimoine, développement international et innovation » au sein du groupe Carrefour ;
M. Jean-Gabriel Ganascia, professeur d'informatique à la faculté des sciences de Sorbonne Université, membre de l'Institut universitaire de France, président du comité d'éthique du CNRS ;
M. Lofred Madzou, responsable de projet « intelligence artificielle et *machine learning* », Centre pour la quatrième révolution industrielle, Forum économique mondial ;
M. Laurent Mucchielli, directeur de recherche au CNRS, laboratoire méditerranéen de sociologie ;
Mme Judith Rochfeld, professeur de droit à l'Université Paris 1 ;
Mme Mélinda Souef, responsable des relations avec le Parlement pour le groupe Aéroports de Paris (ADP).

Contributions

Ambassade de France aux États-Unis : service de la science et de la technologie ;
Ambassade de France au Royaume-Uni : service de la science et de la technologie ;
Ambassade de France aux Pays-Bas : service de sécurité intérieure, service de coopération et d'action culturelle et service de la science et de la technologie.

Références

[1] *Sur ce sujet, voir le rapport (n° 4594) de M. Claude de Ganay et Mme Dominique Gillot, présenté au nom de l'Office en mars 2017, pour une intelligence artificielle maîtrisée, utile et démystifiée.*

http://www.assemblee-nationale.fr/14/rap-off/i4594.asp et sa synthèse
http://www.senat.fr/fileadmin/Fichiers/Images/opecst/quatre_pages/OPECST_rapport_Intelligence_artificielle_synthese_4pages.pdf

[2] *Cette définition du seuil dépend fortement de l'usage qui sera fait de ces dispositifs, le niveau de confiance attendu n'étant pas le même pour une application grand public sur un réseau social, une autorisation d'accès à un site protégé ou un élément de preuve dans une affaire criminelle. L'outil actuellement utilisé par les forces de l'ordre en France propose plusieurs profils pouvant correspondre à l'individu recherché ce qui permet d'augmenter la probabilité d'obtenir une réponse exacte.*

[3] *Deux erreurs peuvent être commises : soit le système ne reconnaît pas l'individu (on parle de faux négatif), soit il reconnaît un individu qui ne devrait pas l'être (on parle alors de faux positif).*

[4] *Note scientifique de l'Office (n° 1) sur les objets connectés :*
http://www2.assemblee-nationale.fr/content/download/65396/664019/version/8/file/note+1+-+4+pages+objets+connectes.pdf

[5] *Une banque a permis l'ouverture d'un compte à distance sans versement obligatoire, en utilisant la reconnaissance biométrique faciale par* selfie *dynamique d'IDEMIA pour identifier le futur client :*
https://www.idemia.com/fr/actualite/societe-generale-et-idemia-revolutionnent-louverture-de-compte-distance-2018-06-01

[6] *Gurovich, Yaron & Hanani, Yair & Bar, Omri & Nadav, Guy & Fleischer, Nicole & Gelbman, Dekel & Basel-Salmon, Lina & M. Krawitz, Peter & Kamphausen, Susanne & Zenker, Martin & M. Bird, Lynne & W. Gripp, Karen. (2019). "*Identifying facial phenotypes of genetic disorders using deep learning" Nature Medicine *25. 10.1038/s41591-018-0279-0 : https://www.nature.com/articles/s41591-018-0279-0*

[7] *L'INRIA et le CMRR du CHU de Nice ont créé en partenariat l'équipe CoBTeK qui étudie ce sujet : http://cmrr-nice.fr/?p=cobtek-presentation*

[8] *Par exemple, la fluidification des flux de passagers dans une gare ou un aéroport peut se faire au passage de certains points d'accès de façon automatisée grâce à des dispositifs de reconnaissance faciale. Ce type d'outil est utilisé dans plusieurs aéroports américains et asiatiques et des entreprises comme Aéroports de Paris (ADP) ou Carrefour ont mené des expérimentations de tels dispositifs.*

[9] *Ces dispositifs sont utilisés dans de nombreux pays afin de contrôler le passage aux frontières, par exemple dans les aéroports ou les gares.*

[10] *Celle-ci n'est qu'un élément d'information et ne constitue en aucun cas une preuve. Article 1er du décret n° 2012-652 :*
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025803463&categorieLien=id

[11] *« Passage automatisé rapide aux frontières extérieures » pour les passagers possédant un passeport biométrique. Le contrôle aux frontières s'effectue dorénavant de façon automatisée pour certains passagers consentants. Le dispositif Parafe contrôle l'identité du voyageur en comparant une photo prise lors du contrôle à celle présente sur son passeport et celle portée par la puce.*

[12] *Avec le soutien de l'Agence nationale des titres sécurisés (ANTS) le ministère de l'intérieur a mis en place, en mai 2019, le système ALICEM (authentification en ligne certifiée sur mobile) permettant à toute personne possesseur d'un téléphone Android et d'un titre sécurisé (passeport, carte de séjour) de disposer d'une identité numérique sécurisée. Dans un avis du 18 octobre 2018, la CNIL avait regretté l'absence d'alternative à la reconnaissance faciale et critiqué la durée de conservation des traces des accès à l'application (6 ans).*

Décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile » : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038475477&categorieLien=id

Avis de la CNIL : https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000038475742

[13] *Dès lors, se pose la question de l'utilisation d'outils de reconnaissance faciale lors des JO qui auront lieu en France en 2024. Il est primordial que le cadre légal d'utilisation soit pérennisé avant cet événement.*

[14] *NIST, Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification, novembre 2018 : https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf*

[15] *https://www.forbes.com/video/5978671815001/#744af9722461*

[16] *Note scientifique de l'Office (n° 2) sur l'impression 3D :*
http://www2.assemblee-nationale.fr/content/download/65485/665121/version/4/file/notescientif_impression+3D+ENG20190409.pdf

[17] *Par exemple le carnaval de Notting Hill au Royaume-Uni (https://www.theguardian.com/uk-news/2018/may/15/uk-police-use-of-facial-recognition-technology-failure) pour lequel la police de Londres a utilisé un dispositif de reconnaissance faciale avec un taux d'erreur de 91 % ; ou l'essai de reconnaissance des conducteurs de voitures à New-York (https://www.wsj.com/articles/mtas-initial-foray-into-facial-recognition-at-high-speed-is-a-bust-11554642000) au cours duquel aucune identification exacte n'a été effectuée.*

[18] *Joy Buolamwini, Timnit Gebru ;* "Proceedings of the 1st Conference on Fairness, Accountability and *Transparency*", PMLR 81:77-91, 2018.
http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

[19] *NIST,* "Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification", juin 2019 :
https://www.nist.gov/sites/default/files/documents/2019/06/20/frvt_report_2019_06_20.pdf

20 Inioluwa Deborah Raji, Joy Buolamwini, "Actionable Auditing : Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products": https://dam-prod.media.mit.edu/x/2019/01/24/AIES-19_paper_223.pdf .
Trois outils étudiés en 2017 (Microsoft, Face++ et IBM) ont fait diminuer leur taux d'erreur concernant les femmes en moyenne de 13 points ; bien que les différences de performance perdurent, les algorithmes étudiés ont en moyenne un taux d'erreur pour les femmes noires supérieur de 15 points à celui pour les hommes blancs.

[21] *Articles 31 et 32 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés :*

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460

[22] *Directive (UE) 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 :*

https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L0680#d1e950-89-1

[23] *En particulier, ces traitements ne sont autorisés que « sous réserve de garanties appropriées pour les droits et libertés de la personne concernée » et uniquement « pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique ; ou lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée ».*

[24] *Commission nationale de l'informatique et des libertés (CNIL).*

[25] *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 (règlement général sur la protection des données, RGPD) : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679*

[26] *Section 3 du chapitre IV du RGPD.*

[27] *Avec l'entrée en vigueur du RGPD, les amendes administratives applicables par les autorités de contrôle ont vu leur plafond considérablement augmenter. Elles peuvent atteindre en cas de récidive jusqu'à 4 % du chiffre d'affaires mondial total et 20 millions d'euros. Article 83(6) du RGPD.*

[28] *L'alinéa 11 de l'article 3 du premier chapitre du RGPD définissant le consentement par « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».*

[29] *Article 8 du RGPD.*

[30] *https://www.lemonde.fr/societe/article/2019/02/18/nice-va-tester-la-reconnaissance-faciale-sur-la-voie-publique_5425053_3224.html*

[31] *La mise au point des algorithmes de reconnaissance faciale nécessite une grande quantité de données. Les dispositions réglementaires actuelles, principalement issues du RGPD, imposent certaines contraintes aux chercheurs et entreprises réalisant des recherches dans ce domaine en Europe. Ce cadre réglementaire ne permet pas à l'heure actuelle aux acteurs français d'être compétitifs sur la scène internationale. Il leur est par exemple impossible d'utiliser des bases d'images recueillies à l'étranger sans le consentement des personnes concernées ou de conserver, après la fin de leur étude, des bases d'images recueillies de façon licite. Ces dispositions représentent donc un véritable frein au développement de ces algorithmes en France et en Europe, les géants du numérique pouvant, en revanche, pour leur part, constituer de très grandes bases d'images sans devoir respecter ces contraintes réglementaires. La CNIL a lancé le 15 juillet 2019 une consultation publique sur ces questions afin de « permettre une meilleure compréhension des traitements de données personnelles dans la recherche scientifique, clarifier le cadre juridique applicable et concevoir des fiches pratiques adaptées ». Il conviendrait également d'étudier la possibilité de mettre en place des dispositions de droit européen ou national permettant de mobiliser les dérogations prévues par le RGPD, afin de permettre aux acteurs de la recherche et de l'innovation en France de bien se positionner dans la compétition internationale.*

https://www.cnil.fr/fr/la-cnil-lance-une-consultation-publique-aupres-des-chercheurs-sur-les-traitements-de-donnees-des

[32] *« Ville sûre »* (safe city)*, adaptation du concept de « ville intelligente »* (smart city) *à la sécurité.*

[33] *https://www.cnil.fr/fr/la-cnil-appelle-la-tenue-dun-debat-democratique-sur-les-nouveaux-usages-des-cameras-video*

[34] *https://www.laquadrature.net/2019/06/21/le-vrai-visage-de-la-reconnaissance-faciale/*

[35] *https://www.lesechos.fr/tech-medias/hightech/en-chine-la-vie-sous-loeil-des-cameras-997774*

[36] *https://www.lemonde.fr/asie-pacifique/article/2018/04/11/en-chine-le-fichage-high-tech-des-citoyens_5283869_3216.html*

https://www.franceinter.fr/monde/la-chine-distribue-des-bons-et-des-mauvais-points-a-ses-citoyens

[37] *http://www.lefigaro.fr/flash-actu/pekin-utilise-la-reconnaissance-faciale-pour-surveiller-les-ouighours-presse-20190415*

[38] *Laurent Mucchielli précise : « les nouvelles technologies de manière générale, et les technologies de sécurité en particulier, sont l'objet de croyances et d'imaginaires collectifs très puissants dans nos sociétés actuelles. Ceci favorise une sorte de crédulité et de naïveté générales conduisant à penser spontanément que les innovations technologiques proposées par les industriels et certains politiques sont nécessairement bonnes ou intéressantes en soi ;; ce serait forcément* le progrès*. Or ces raisonnements sont viciés. La technologie n'est ni bonne ni mauvaise en soi. Tout dépend des usages que nous décidons d'en faire et des arbitrages financiers qui sont faits derrière nos choix ». Extraits de « Note sur l'évaluation des nouvelles technologies de sécurité. Cas de la vidéosurveillance et de la reconnaissance faciale » : https://halshs.archives-ouvertes.fr/halshs-02178394 .*

[39] *La première réunion, à laquelle le rapporteur a participé, s'est déroulée le 26 juin 2019. https://cnnumerique.fr/regulation_reconnaissance_faciale*

[40] *https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/*

[41] *Par exemple, Microsoft s'engage à développer des outils de reconnaissance faciale de façon transparente en intégrant des organismes indépendants dans le contrôle de ses algorithmes et en mettant les résultats à disposition du public : https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/*

[42] *Pour sa part, le géant du net a ainsi pris l'engagement de garantir l'excellence scientifique des dispositifs qu'il met au point et de ne pas renforcer les biais de la société. Google Cloud a de plus fait le choix de ne pas proposer d'outil de reconnaissance faciale à usage général avant d'avoir résolu certaines questions d'ordre techniques ou relevant des conditions d'utilisation de ces dispositifs :*

https://blog.google/technology/ai/ai-principles/ ; https://www.blog.google/around-the-globe/google-asia/ai-social-good-asia-pacific/

[43] *À l'heure actuelle rien ne prouve qu'il est impossible de reconstituer (« déflouter ») le visage original grâce à des traitements vidéos plus ou moins sophistiqués. https://brighter.ai/*

[44] *En effet, ces outils nécessitent d'être complétés pour devenir opérationnels, la responsabilité se reportant donc, selon Amazon, sur l'intégrateur et le responsable de traitement.*

[45] *Les États-Unis déploient actuellement plusieurs projets de recherche dans ce domaine : contrôle à l'entrée des bases militaires, viseur « intelligent », drones… : https://www.military.com/daily-news/2019/06/01/armys-next-infantry-weapon-could-have-facial-recognition-technology.html*

[46] *La police britannique utilise dès à présent la reconnaissance faciale dans le domaine public afin de retrouver un certain nombre de personnes recherchées. Il a été estimé que l'utilisation généralisée de l'identification faciale coûterait 500 millions de livres (environ 550 millions d'euros), soit 10 livres par personne identifiés. L'utilisation de ces technologies ne se restreint pas à la sécurité intérieure, mais également à la sécurisation de l'accès aux services financiers et gouvernementaux, ou encore de certains aéroports.*

[47] *En plus de l'expérimentation au carnaval de Notting Hill, le MPS a également mené une expérimentation dans la station très fréquentée de Stratford.*

[48] *Cette stratégie limite les cas dans lesquels la reconnaissance faciale peut être utilisée (maintien de l'ordre, contrôle des passeports et sécurité nationale en cas de législation afférente) et s'accompagne de la mise en place d'organismes de régulation indépendants comme le récent* Law Enforcement

Facial Images and New Biometrics Oversight and Advisory Board, *encadrant pour sa part l'utilisation de cette technologie par les forces de l'ordre.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf

[49] Parliamentary Office of Science & Technology (POST): https://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-0578

[50] *Le* Commercial Facial Recognition Privacy Act *(https://www.congress.gov/bill/116th-congress/senate-bill/847/text) a pour objectif d'encadrer les utilisations commerciales de la reconnaissance faciale, de contrôler les performances des dispositifs mis sur le marché et d'imposer aux entreprises d'obtenir le consentement des individus.*

[51] *Ces expérimentations devaient ensuite permettre de mettre au point un cadre légal pérenne opérationnel au plus tard lors des Jeux Olympiques de 2024 à Paris, qui pourraient servir de vitrine grandeur nature.*

[52] *Privacy by design : garantie que la protection de la vie privée soit intégrée dans les nouvelles applications dès leur conception..*

[53] *Dans le domaine de la téléphonie, l'Autorité de régulation des communications électroniques et des postes (ARCEP) a mis en place un dispositif de « bac à sable », donnant la possibilité à certains acteurs de mener des expérimentations en dérogeant à certaines règles.*

[54] *Rapport de Cédric Villani, parlementaire en mission, au Premier ministre : « Donner un sens à l'intelligence artificielle, pour une stratégie nationale et européenne » (mars 2018).*

https://www.aiforhumanity.fr/