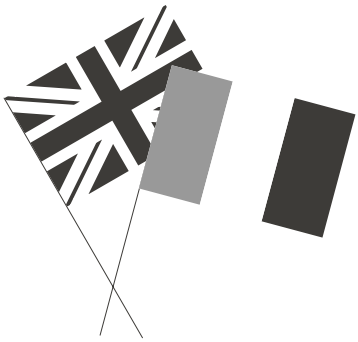
RENAISSANCE numerique

LIBERTÉS PUBLIQUES ET ÉTHIQUE
JUIN 2021

Encadrement des technologies de reconnaissance faciale :

UNE ANALYSE COMPARÉE DE LA FRANCE ET DU ROYAUME-UNI



Le 21 avril 2021, la Commission européenne dévoilait sa proposition de règlement visant à encadrer les usages variés des technologies d'intelligence artificielle (IA) au sein de l'Union européenne, dont font notamment partie les technologies de reconnaissance faciale[1]. Ces dernières reposent sur des méthodes d'intelligence artificielle qui appliquent des techniques dites d'apprentissage profond (*deep learning*), en s'appuyant sur des bases de données biométriques. Elles peuvent être utilisées à des fins d'authentification (par exemple, vérifier une identité à partir d'un visage donné) et d'identification (par exemple, associer une identité à un visage donné parmi une base de données de visages connus). Les technologies de reconnaissance faciale sont entrées dans le quotidien des citoyens européens à différentes échelles et par le biais de différentes expériences, comme la possibilité de déverrouiller son smartphone avec son visage ou d'identifier automatiquement des amis sur des photos publiées sur un réseau social. Les applications en sont nombreuses, ces technologies pouvant être utilisées tout autant à des fins de sécurité (sécurité aux frontières, déverrouillage d'un smartphone, paiements en ligne, accès à des services publics…), de marketing (publicité ciblée), voire même récréatives (*face swapping*, identification sur des photographies sur les réseaux sociaux)[2].

Dans sa proposition de règlement, la Commission européenne opte pour une approche fondée sur les risques en catégorisant les solutions d'IA selon qu'elles comportent un degré de risque inacceptable, élevé, ou faible. Ainsi, quatre pratiques en matière d'IA sont interdites par la proposition, la Commission considérant qu'elles

1 Commission européenne, "Proposal for a Regulation of the european Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Unions Legislative Acts", COM(2021) 206 final, 21 avril 2021 : https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence

2 Pour de plus amples informations, voir Renaissance Numérique (2020), « Reconnaissance faciale : Porter les valeurs de l'Europe », 103 pp. : https://www.renaissancenumerique.org/system/attach_files/files/000/000/231/original/Rapport_Reconnaissance_Faciale.pdf?1591797462

comportent un degré de risque inacceptable. C'est le cas notamment de l'identification biométrique en temps réel et à distance dans l'espace public par les forces de l'ordre (article 5(1)(d)). L'exécutif européen juge, en effet, cet usage contraire aux valeurs de l'Union européenne[3]. Cette interdiction comporte toutefois trois exceptions, relativement larges, prévues par le texte. Les forces de police pourront, par exemple, utiliser ces technologies pour rechercher des victimes d'actes criminels, incluant les enfants disparus, pour localiser une victime ou un suspect d'une infraction pénale passible d'une peine privative de liberté d'au moins trois ans, ou encore pour prévenir une menace pour la vie ou la sécurité d'autrui ou en cas d'attaque terroriste. Quant aux autres usages des solutions d'IA impliquant une identification biométrique à distance – par exemple, les usages dans le secteur privé –, la Commission européenne propose de les classer dans la catégorie des applications à risque élevé[4]. À ce titre, leur usage serait soumis au respect de certaines garanties, notamment la mise en place d'un système de gestion des risques (article 9), un niveau minimal de qualité des données utilisées pour entraîner les algorithmes (article 10), un devoir de transparence et d'information vis-à-vis des utilisateurs (article 13) et une supervision humaine (article 14).

La nécessité d'encadrer le déploiement des technologies de reconnaissance faciale afin de protéger les droits et libertés fondamentaux des citoyens européens est au cœur des débats. Leur caractère hautement intrusif est de plus en plus dénoncé par certains acteurs de la société civile, comme ceux à l'origine de la campagne *Reclaim Your Face*[5]. Si le traitement de données biométriques est, en principe, interdit par le Règlement général sur la protection des données (RGPD)[6], ce dernier comporte, en effet, de nombreuses exceptions. Dans un rapport publié en juin 2020[7], Renaissance Numérique a, à ce sujet, relevé que, malgré l'existence d'un cadre juridique particulièrement fourni, son application demeure disparate et peu efficiente, mettant ainsi en danger les droits des citoyens européens.

Dans la continuité de ses travaux, le think tank a organisé un séminaire, le 21 février 2021, visant à établir une analyse comparative de l'utilisation des technologies de reconnaissance faciale entre deux pays européens : la France et le Royaume-Uni. Préparé en partenariat avec l'Ambassade du Royaume-Uni à Paris et le cabinet d'avocats Pinsent Masons, ce séminaire européen a réuni une cinquantaine d'acteurs privés et publics, de la société civile et du monde de la recherche. La comparaison de la France et du Royaume-Uni vis-à-vis des usages et de l'encadrement des technologies de reconnaissance faciale revêt plusieurs intérêts. D'une part, les débats sont désormais relativement ancrés (bien que récents) dans les deux pays. D'autre part, il existe des variations notables dans la manière de déployer et réguler ces technologies de part

3 Commission européenne, *op. cit.*, p. 12.
4 *Ibid.*, Annexe III, p.4.
5 Voir : https://reclaimyourface.eu/
6 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 : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679
7 Renaissance Numérique (2020), *op. cit.*

et d'autre de la Manche.

Cette note, nourrie de ces échanges, interroge les principaux enjeux que soulève l'encadrement des technologies de reconnaissance faciale en France, au Royaume-Uni, et plus largement en Europe. Une comparaison qui permet de dessiner les lignes d'une régulation idoine pour répondre aux défis posés par ces technologies.

Un encadrement des technologies de reconnaissance faciale tributaire de la culture juridique du pays

En France comme au Royaume-Uni, les technologies de reconnaissance faciale sont utilisées à la fois dans les espaces publics et privés et à la fois par des acteurs publics ou privés. En France, la puissance publique a, par exemple, recours à ces technologies pour le traitement des antécédents judiciaires (TAJ), le passage rapide aux frontières extérieures (via le système PARAFE), et l'authentification en ligne certifiée sur mobile (ALICEM)[8] qui permet d'accéder à des services publics en ligne. Des expérimentations de ces technologies à des fins sécuritaires ont également été menées dans les territoires, comme ce fut le cas lors du carnaval de Nice en février 2019[9], ou dans le cadre du contrôle de l'accès à deux lycées dans la région PACA[10]. À Marseille, des technologies de reconnaissance faciale reposant sur un réseau d'une cinquantaine de caméras de vidéoprotection ont été déployées[11], avant que le projet ne soit finalement suspendu début 2021[12]. Des usages qui divisent et contre lesquels se sont mobilisées plusieurs associations de défense des droits, dont la Quadrature du Net et la Ligue des droits de l'Homme. Contrairement aux usages déployés en France, qui relèvent pour partie d'expérimentations, des outils de reconnaissance faciale pour la surveillance ont été utilisés à grande échelle et sur la base de vraies bases de données biométriques outre-Manche, soulevant des inquiétudes vis-à-vis de la protection de la vie privée, notamment en termes de recueil du consentement des individus dont les visages sont scannés. L'affaire du quartier de King's Cross à Londres en 2019 a ainsi révélé que les passants étaient filmés à leur insu par un promoteur immobilier,

8 Pour de plus amples informations sur le fonctionnement d'ALICEM : https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Alicem-la-premiere-solution-d-identite-numerique-regalienne-securisee

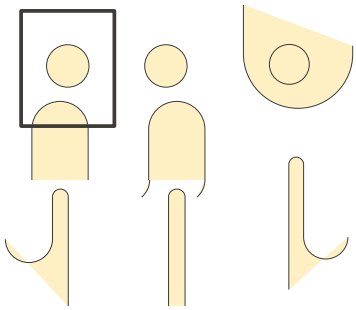
9 « Nice: La reconnaissance faciale testée sur la voie publique, au Carnaval, une première en France », *20 minutes*, 18 février 2019 : https://www.20minutes.fr/nice/2454127-20190218-video-nice-reconnaissance-faciale-testee-carnaval-premiere-france

10 « Deux lycées de Marseille et Nice vont tester la reconnaissance faciale », *Le Figaro*, 17 décembre 2018 : https://www.lefigaro.fr/actualite-france/2018/12/17/01016-20181217ARTFIG00207-deux-lycees-de-marseille-et-nice-vont-tester-la-reconnaissance-faciale.php

11 « Marseille : la vidéoprotection « intelligente », comment ça marche », *France 3 Provence Alpes Côte d'Azur*, 5 février 2021 : https://france3-regions.francetvinfo.fr/provence-alpes-cote-d-azur/bouches-du-rhone/marseille/marseille-la-videoprotection-intelligente-comment-ca-marche-1941052.html

12 La nouvelle majorité municipale, qui n'est pas à l'origine du projet, a suspendu ce dernier le temps que soit organisé un audit visant à déterminer la pertinence et l'efficacité du système.

qui communiquait avec la police des informations en vue d'identifier des personnes fichées. L'autorité de protection des données britannique, l'*Information Commissioner's Office* (ICO)[13], enquête actuellement sur l'utilisation qui a été faite de la reconnaissance faciale[14] dans ce cas précis, et a appelé le gouvernement à adopter un code de bonne conduite sur ce genre d'usages[15]. Ces technologies y sont également plus souvent utilisées par des acteurs privés, à l'instar de certains supermarchés, où les visages des personnes entrant sont scannés et comparés à des listes de suspects. Des dispositifs de reconnaissance faciale ont également été déployés au cours d'événements rassemblant un grand public, par exemple lors de concerts ou de matchs de rugby et de football, comme lors de la finale de l'UEFA à Cardiff en 2017.



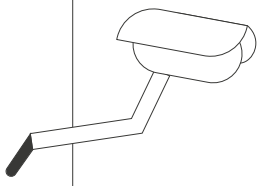
Face au développement de ces usages, un débat public commence à émerger de part et d'autre de la Manche sur l'encadrement de ces technologies. Au Royaume-Uni, ce dernier est relativement récent et a été interrompu par la crise du Covid-19. Un projet de loi a notamment été déposé le 4 février 2020 par le sénateur Lord Clement-Jones. Ce dernier vise à interdire l'utilisation des technologies de reconnaissance faciale automatisée dans les lieux publics et demande à ce qu'une évaluation de ces technologies soit réalisée par un panel indépendant sous un an. L'évaluation devrait en outre couvrir les aspects suivants : les implications de l'utilisation de ces technologies en matière d'égalité et de droits humains, en matière de protection des données, la qualité et la précision de ces technologies, et l'adéquation du cadre réglementaire existant. Ce texte est actuellement en seconde lecture à la Chambre des Lords[16]. Il concerne toutefois exclusivement l'usage public (et non privé) des technologies de reconnaissance faciale. Les cas d'usage sont donc traités séparément, et il n'existe pas, à ce jour, de politique globale sur la question au Royaume-Uni.

En France, le débat s'intensifie à l'approche d'échéances sportives internationales, comme l'organisation de la coupe du monde masculine de rugby en 2023 et des Jeux olympiques de Paris en 2024. Les technologies de reconnaissance faciale sont envisagées par les organisateurs de ces événements afin de sécuriser l'accès aux différentes installations sportives[17], ce qui ouvrirait la voie à des expérimentations à plus grande échelle que ce qui n'a été fait jusqu'à présent. À ce titre, la Commission nationale de l'informatique et des libertés (CNIL) n'exclut pas de rendre un avis favorable à l'utilisation de tels dispositifs à des fins sécuritaires lors des Jeux olympiques[18], à certaines conditions. Le sujet a toutefois été laissé en marge de la proposition de loi dite « Sécurité globale », la majorité parlementaire étant divisée quant à l'utilisation de ces tech-

13 Voir le site de l'ICO : https://ico.org.uk/about-the-ico/
14 ICO, "Statement: Live facial recognition technology in King's Cross", 15 août 2019 : https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/
15 ICO, "ICO investigation into how the police use facial recognition technology in public places", 31 octobre 2019, pp. 36-37 : https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf
16 UK House of Lords, "Automated Facial Recognition Technology (Moratorium and Review) Bill", 4 février 2020 : https://bills.parliament.uk/bills/2610
17 « Reconnaissance faciale : les expérimentations se multiplient avant les J.O de Paris », *Radio France*, 5 septembre 2020 : https://www.francetvinfo.fr/economie/emploi/metiers/armee-et-securite/reconnaissance-faciale-les-experimentations-se-multiplient-avant-les-j-o-de-paris_4095193.html
18 *Ibid.*

nologies.[19] Dans ce contexte, le député Didier Baichère a présenté au début du mois de mai 2021 une proposition de loi « d'expérimentation et de consultation sur les dispositifs de reconnaissance faciale par l'intelligence artificielle »[20]. Ce texte vise à établir un cadre d'expérimentation « transparent et éthique » pour les technologies de reconnaissance faciale qui mobilisent l'IA. Il prévoit également l'organisation d'une consultation citoyenne, dans le but de « *faire naître les conditions d'un débat citoyen et pédagogique pour éclairer et mesurer les perceptions des Français et détecter les lignes rouges à ne pas franchir.* »[21] Au-delà de ces échéances nationales, tout l'enjeu en France dans les mois à venir sera d'intégrer l'approche européenne préconisée par le futur règlement sur l'IA.

Bien que les cas d'usages de ces technologies soient multiples (usages sécuritaires, mais aussi à des fins marketing, voire récréatives), les débats tendent ainsi à se focaliser sur le recours de ces dernières à des fins de surveillance (les autres usages n'étant pourtant pas dépourvus de risque). C'est d'ailleurs sur cet aspect que se sont concentrées les discussions lors du séminaire du 21 février 2021. À cet égard, il a été souligné lors de l'événement, que les autorités françaises se sont montrées jusqu'à présent plus prudentes que le Royaume-Uni quant au déploiement de ces technologies à des fins de surveillance. Alors que le Royaume-Uni est le premier pays d'Europe à recourir à des bases de données biométriques réelles pour ses usages de la reconnaissance faciale dans l'espace public, le déploiement de ces technologies repose en France quasi-exclusivement sur des expérimentations limitées dans le temps et dans l'espace. En outre, ces expérimentations n'ont lieu qu'avec le consentement des personnes concernées. Ce fut, par exemple, le cas en février 2019 à l'occasion du Carnaval de Nice[22]. Le Conseil d'État a, par ailleurs, récemment interdit l'usage de drones embarquant des dispositifs de reconnaissance faciale dans l'espace public à des fins de contrôle du respect du confinement dans le cadre de la lutte contre le Covid-19[23]. Le tribunal administratif de Marseille s'est également aligné sur la position de la CNIL[24] défavorable au contrôle d'accès virtuel expérimenté à l'entrée de deux lycées de Marseille et Nice, arguant que d'autres systèmes de contrôle tout aussi efficaces existaient[25].



19 « Les Jeux olympiques ouvrent la voie aux technologies sécuritaires », *Reporterre*, 16 mars 2021 : https://reporterre.net/Les-Jeux-olympiques-ouvrent-la-voie-aux-technologies-securitaires

20 Assemblée nationale, « Proposition de loi d'expérimentation créant un cadre d'analyse scientifique et une consultation citoyenne sur les dispositifs de reconnaissance faciale par l'intelligence artificielle », 4 mai 2021 ; https://www.assemblee-nationale.fr/dyn/15/textes/l15b4127_proposition-loi.pdf

21 Didier Baichère, communiqué de presse, « Publication de ma proposition de loi d'expérimentation et de consultation sur les dispositifs de reconnaissance faciale par l'intelligence artificielle », 7 mai 2021 : https://www.didierbaichere.fr/blog/publication-de-ma-proposition-de-loi-d-experimentation-reconnaissance-faciale

22 « Expérimentation de reconnaissance faciale : Nice ravie, la Cnil sceptique », *Le Journal du Net*, 28 août 2019 : https://www.journaldunet.com/economie/services/1443319-reconnaissance-faciale-nice-ravie-la-cnil-sceptique/.

23 Conseil d'État, « Avis relatif à l'usage de dispositifs aéroportés de captation d'images par les autorités publiques », 18 juillet 2020 : https://www.conseil-etat.fr/ressources/avis-aux-pouvoirs-publics/derniers-avis-publies/avis-relatif-a-l-usage-de-dispositifs-aeroportes-de-captation-d-images-par-les-autorites-publiques

24 CNIL, Avis sur l'expérimentation de la reconnaissance faciale dans deux lycées, 17 octobre 2019 : https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position

25 Tribunal administratif de Marseille, 9e ch., jugement du 27 février 2020 : https://www.legalis.net/jurisprudences/tribunal-administratif-de-marseille-9eme-ch-jugement-du-27-fevrier-2020/

Il semblerait que les autorités françaises soient plus réticentes que leurs homologues britanniques, quant à l'utilisation des technologies de reconnaissance faciale à des fins sécuritaires. Il ressort, en effet, des échanges entre les participants au séminaire, que lorsque la justice britannique est venue condamner une pratique, elle le faisait généralement pour des motifs qui tenaient davantage aux conditions liées à l'utilisation des données à caractère personnel ou au non-respect du principe de discrimination, plutôt qu'à l'utilisation des technologies de reconnaissance faciale à des fins sécuritaires en tant que telles. C'est notamment ce qui ressort de la décision rendue par la Cour d'appel du Royaume-Uni sur l'usage des technologies de reconnaissance faciale par la police du sud du Pays de Galles[26]. Dans cette affaire, un argument rappelé par l'ICO dans son rapport d'investigation était que la collecte des données devait être adéquate, pertinente et proportionnée, ce qui n'était pas le cas ici, car la police du sud du Pays de Galles utilisait des listes de suspects particulièrement larges[27]. Si la Cour d'appel a jugé que la police avait eu tort de considérer que les données de personnes hors des listes de surveillance étaient publiques, elle a toutefois relevé l'intérêt de l'utilisation des technologies de reconnaissance faciale[28].

Les autorités britanniques ont parfois une lecture moins rigoriste du RGPD que les autorités françaises au sujet du recours aux technologies de reconnaissance faciale à des fins de surveillance, et en particulier en ce qui concerne le respect du principe de proportionnalité. Ainsi, au Royaume-Uni, si les données biométriques sont collectées pour un usage spécifique, sur un temps limité et dans une zone géographique donnée et que ces données sont ensuite effacées, alors l'utilisation des technologies de reconnaissance faciale est généralement autorisée. Cette approche entraîne des décisions juridiques plus souples au Royaume-Uni et témoigne de la différence de culture d'encadrement sur ces questions entre les deux pays.

Au-delà de ces aspects juridiques propres à l'utilisation de ces technologies, des différences culturelles plus larges transparaissent également. Les dispositifs de vidéosurveillance sont, par exemple, beaucoup plus développés au Royaume-Uni qu'en France, bien que le pays ait connu également un essor considérable de ces dispositifs. Enfin, l'organisation décentralisée du Royaume-Uni entraîne parfois une hétérogénéité des approches sur ces questions entre les différents territoires. Par exemple, l'Écosse est plus réticente que l'Angleterre à utiliser les technologies de reconnaissance faciale dans le cadre de ses pouvoirs de police[29], au nom du principe de précaution.

---

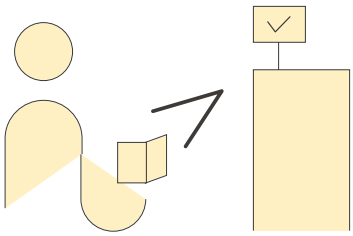
26 Court of appeal, R (Bridges) v-Chief Constable of South Wales Police & Ors, 11 août 2020 : https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

27 ICO, "ICO investigation into how the police use facial recognition technology in public places", 31 octobre 2019, pp. 16-17 et p. 25 : https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

28 *Ibid*., p. 30.

29 "Facial recognition: 'No justification' for Police Scotland to use technology", *BBC*, 11 février 2020: https://www.bbc.com/news/uk-scotland-51449166

Le recours aux technologies de reconnaissance faciale nécessite des garde-fous qui vont au-delà de critères techniques



Afin de réguler au mieux les technologies de reconnaissance faciale en fonction de la place que l'on souhaite leur accorder dans la société, les risques et les opportunités offerts par ces dernières doivent être clairement identifiés. Comme évoqué par certains participants au séminaire, elles présentent *a priori* des avantages. Les données biométriques ne peuvent pas être facilement piratées. Elles ne peuvent pas non plus être oubliées, contrairement à un mot de passe. En cela, leur utilisation diminue le risque d'usurpation d'identité dans le cadre de démarches administratives et bancaires en ligne. D'autre part, les technologies de reconnaissance faciale seraient particulièrement efficaces pour certaines tâches, comme l'authentification de personnes aux frontières ou pour l'usage de services bancaires en ligne. Ainsi, leur sécurité et leur fiabilité sont deux arguments qui reviennent souvent pour justifier leur recours.

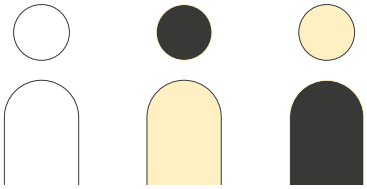
Cependant, la nature même des technologies de reconnaissance faciale peut entraîner de nombreux risques, la précision des algorithmes sur lesquels elles reposent n'étant jamais fiable à 100 %. Plusieurs études ont d'ailleurs révélé que ces derniers reproduisent les nombreux biais[30] (racistes, sexistes ou âgistes) observés dans la société, entrainant ainsi des risques de discrimination importants, comme le non-accès à un service par erreur, ou une arrestation abusive. Ainsi, même si l'efficacité technique des technologies de reconnaissance faciale est régulièrement mise en avant par les acteurs qui les utilisent, ces technologies ne sont (et ne seront) jamais complètement fiables.

Quand bien même elles le seraient, et ne comporteraient aucun biais, y recourir soulève des enjeux qui vont au-delà de simples aspects techniques. Selon leur usage, sont soulevées, en effet, de sérieuses interrogations quant à leur compatibilité avec les droits et libertés fondamentaux des individus à qui elles s'appliquent, notamment en termes de légalité, de nécessité et de proportionnalité. L'une des difficultés majeures que soulève l'utilisation de ces technologies est la question du consentement des individus, particulièrement difficile à obtenir dans les espaces publics. L'obligation de transparence et d'information des citoyens sur le fait que leurs données biométriques sont susceptibles d'être collectées apparaît, à ce titre, essentielle. Bien qu'il existe au Royaume-Uni un cadre légal visant à protéger les données personnelles des

30 Voir par exemple le projet "Gender Shades" développé par le Massachusetts Institute of Technology, 2018 : http://gendershades.org/overview.html

individus[31], des difficultés d'application de ces différentes lois peuvent subsister. De plus, elles ne traitent pas de tous les cas qui peuvent exister de manière exhaustive, comme la question de la confidentialité des données biométriques dans des situations à risque.

Mal utilisées, les technologies de reconnaissance faciale peuvent porter atteinte à la dignité humaine par leur caractère intrusif, ainsi qu'à d'autres principes tels que le droit à la non-discrimination, la liberté d'expression et d'association, ou encore le droit à une bonne administration[32]. La performance technique des systèmes de reconnaissance faciale n'est donc pas un critère suffisant pour justifier la nécessité et la proportionnalité de leur utilisation. Des garde-fous doivent être pensés, qui vont au-delà de critères techniques tels que le degré de précision des algorithmes, afin de garantir la protection des droits et libertés fondamentaux des citoyens.

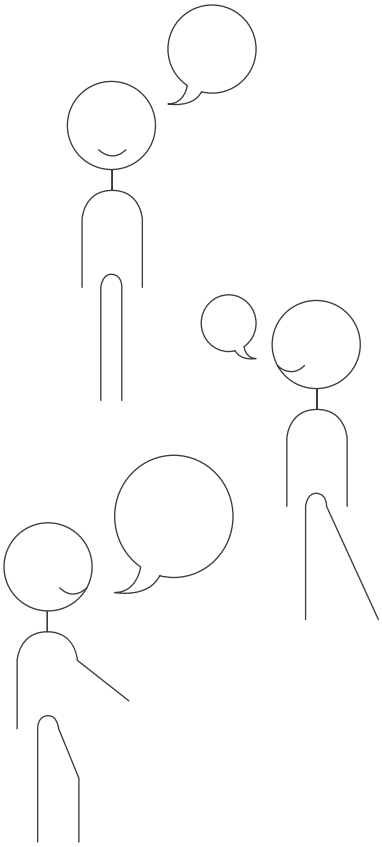


Lors du séminaire, des participants ont évoqué que ces garde-fous pourraient prendre la forme d'organismes de contrôle indépendants, chargés d'évaluer la qualité des dispositifs de reconnaissance faciale (à la fois en amont et en aval de leur utilisation), de mettre en place des contrôles et procédures d'autorisation de leur utilisation, et de réguler la collecte et l'utilisation de données biométriques. Il ressort également des discussions qu'au vu de la sensibilité de ces technologies et de la grande variété de cas d'usages possibles, une analyse *a priori* et au cas par cas devrait être envisagée. Parmi les arguments mis en avant, ressort l'idée qu'un tel cadre d'évaluation des risques permettrait d'aller plus loin que les analyses d'impact relatives à la protection des données (AIPD) prévues par le RGPD. L'approche mise en avant par la Commission européenne dans sa proposition de règlement sur l'IA va d'une certaine manière en ce sens. L'exécutif européen suggère que les systèmes d'IA visant l'identification biométrique à distance de personnes physiques fassent l'objet d'une procédure d'évaluation de conformité *ex ante* par un organisme notifié.

Cependant, il n'existe pour l'heure en Europe pas de consensus quant aux organismes qui devraient idéalement être chargés de ces évaluations et comment ils devraient remplir cette mission. Il convient de noter toutefois que pour être efficaces, ces organismes devraient être indépendants et non biaisés, et devraient émettre des avis clairs et univoques, qui ne puissent pas être soumis à des différences d'interprétation.

31 Parmi les plus importantes, on retrouve le *Human Rights Act* de 1998, l'*Investigatory Powers Act* de 2016 ou encore le *Data Protection Act* de 2018.

32 European Union Agency for Fundamental Rights, "Facial recognition technology: fundamental rights considerations in the context of law enforcement", 21 novembre 2019, 34 pp.: https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law



L'encadrement des technologies de reconnaissance faciale doit prendre en compte leur impact collectif sur la société

L'utilisation des technologies de reconnaissance faciale a des incidences sur l'ensemble de la société. Dès lors, leur encadrement doit être pensé au-delà de leur impact individuel, qui est essentiellement traité sous le prisme de la protection des données personnelles. Pour combler le manque d'implication des citoyens dans la décision publique au Royaume Uni, une initiative a été lancée par l'Ada Lovelace Institute, un centre de recherche indépendant qui s'est penché sur la question des technologies biométriques et de reconnaissance faciale. Selon une étude réalisée en septembre 2019 par cet institut, 55% des citoyens interrogés souhaitent des restrictions sur l'utilisation de ces technologies par les forces de police[33], et une part importante de la société distingue des usages légitimes d'autres usages jugés illégitimes, comme le fait d'utiliser la reconnaissance faciale dans les transports en commun ou dans les écoles. Face à ce constat, l'Ada Lovelace Institute a créé le *Citizen's Biometric Council* [34] , un conseil délibératif composé d'une cinquantaine de citoyens représentatifs de la société britannique. Au travers de nombreux débats avec des experts, les membres de ce conseil ont proposé un ensemble de mesures visant à rendre l'utilisation des technologies biométriques «digne de confiance»: instaurer une législation et une réglementation plus poussées, mettre en place un organisme indépendant et faisant autorité pour assurer une surveillance rigoureuse, garantir des standards *minimum* en matière de conception et de déploiement[35].

Cet exemple montre que le partage d'informations et la participation aux débats permettent aux citoyens de faire des choix de société éclairés. Informer le public apparaît donc comme une priorité, ainsi que la mise en place de processus délibératifs, où professionnels des technologies de reconnaissance faciale, chercheurs, représentants de la société civile, régulateurs et citoyens seraient invités à discuter et confronter leurs avis.

33 Ada Lovelace Institute, "Beyond face value: public attitudes to facial recognition technology", septembre 2019, 23 pp.: https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/

34 Voir la présentation du "Citizens' Biometrics Council" sur le site web de l'institut Ada Lovelace: https://www.adalovelaceinstitute.org/project/citizens-biometrics-council/

35 Ada Lovelace Institute, "The Citizens' Biometrics Council — Recommendations and findings of a public deliberation on biometrics technology, policy and governance", mars 2021, p. 3: https://www.adalovelaceinstitute.org/wp-content/uploads/2021/03/Citizens_Biometrics_Council_final_report.pdf

Vers un débat ouvert et multipartite

L'étude comparative de la France et du Royaume-Uni en ce qui concerne le déploiement et l'encadrement des technologies de reconnaissance faciale révèle des différences d'usages entre ces deux pays, qui relèvent tant d'aspects politiques, que juridiques ou socioculturels. Il apparaît primordial que l'encadrement de ces technologies ne se fonde pas uniquement sur leur efficience technique, mais aussi sur le respect des droits et libertés fondamentaux des citoyens. À cet égard, une évaluation au cas par cas par des organismes indépendants pourrait constituer une partie de la solution. Alors que la Commission européenne vient de proposer son règlement visant à encadrer diverses technologies d'IA, et que ce dernier autorise plusieurs usages des technologies de reconnaissance faciale, le moment est venu de structurer une vision collective quant à l'encadrement de ces dernières.

—

Rédaction

Jessica Galissaire, Responsable des études, Renaissance Numérique

Audrée Latinaud, Chargée de mission, Renaissance Numérique

—

Relecture

Jennyfer Chrétien, Déléguée générale, Renaissance Numérique

Guillaume Morat, Avocat associé, Pinsent Masons

—

Renaissance Numérique tient à remercier l'Ambassade du Royaume-Uni à Paris et le cabinet Pinsent Masons pour leur soutien dans l'organisation du séminaire «Facial Recognition Technologies: Comparative views from across the Channel» le 11 février 2021.

Le think tank remercie également l'ensemble des participants au séminaire, qui ont nourri la réflexion de la présente note, et en particulier Tom Barry, Minister Counsellor pour les affaires européennes et internationales à l'Ambassade du Royaume-Uni à Paris, Théodore Christakis, Professeur de droit et titulaire de la chaire sur les implications juridiques et réglementaires de l'IA à l'Université Grenoble-Alpes, Benedict Dellot, Responsable de la surveillance de l'IA au Centre for Data Ethics & Innovation, Claire Edwards, Avocate associée chez Pinsent Masons, Stéphanie Hare, Chercheuse spécialisée dans les questions *tech*, Irina Orssich, Responsable IA au sein de l'unité «Développement et coordination des politiques en matière d'intelligence artificielle» à la DG CNECT de la Commission européenne, Hetan Shah, Vice-président de l'Ada Lovelace Institute et Camille Vaziaga, Responsable des Affaires publiques France chez Microsoft.