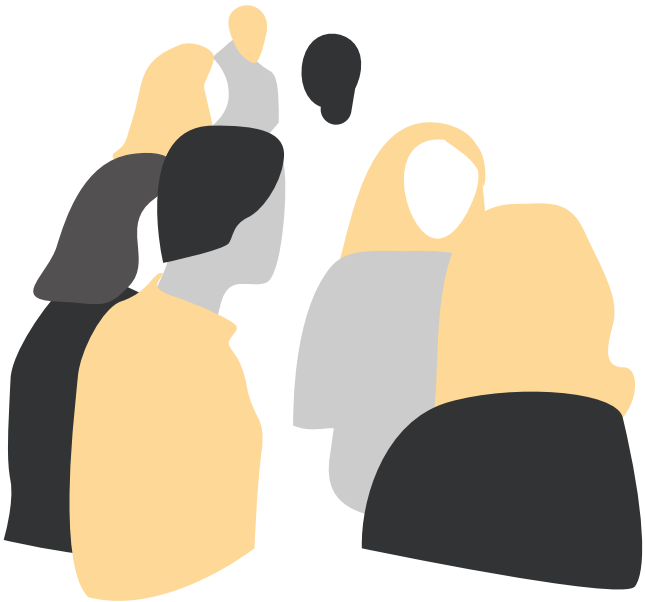
ACTES DU COLLOQUE DU 19 DÉCEMBRE 2019

Reconnaissance faciale : Interdiction, expérimentation, généralisation, réglementation. Où en est-on ? Où allons-nous ?

LIBERTÉS PUBLIQUES ET ÉTHIQUE

FÉVRIER 2020

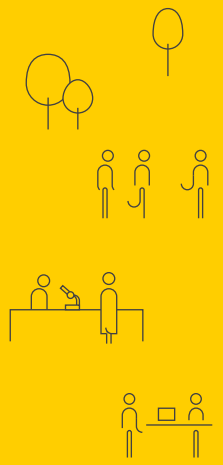
RENAISSANCE numerique



PRÉAMBULE

Les technologies de reconnaissance faciale, fondées sur le déploiement exponentiel des technologies d'intelligence artificielle, se développent de plus en plus dans la vie quotidienne, notamment pour la sécurisation de certains accès (déverrouiller un service, accéder à un compte bancaire, accéder à des locaux, etc.), non sans susciter des interrogations et des craintes sur la généralisation de ces usages.

Alors que les acteurs institutionnels s'interrogent sur la robustesse du cadre juridique actuel, les associations, au nom de la défense des droits et libertés fondamentales, et les entreprises souhaitent évoluer dans un cadre serein et sécurisé. Il est nécessaire de prendre le temps du débat et de rassembler les différentes parties prenantes proposant des retours d'expérience et un positionnement sur ces enjeux.



Dans ce cadre, le think tank Renaissance Numérique et Jean-Michel Mis, Député de la Loire ont organisé un colloque dédié à ces enjeux, le jeudi 19 décembre 2019 à l'Assemblée nationale. Cette rencontre visait à rassembler acteurs publics, privés, de la société civile et du monde de la recherche, pour réfléchir de manière approfondie aux usages de la reconnaissance faciale, à ses enjeux en termes de droits et libertés fondamentales ainsi qu'à son encadrement juridique et les perspectives d'évolution.

Ce cahier rapporte les propos qui se sont tenus lors de cet après-midi de débats de la manière la plus exhaustive possible, à l'exception de la restitution de l'enquête conduite par Renaissance Numérique et l'Ifop qui a déjà fait l'objet d'une publication (voir la référence à la fin de ce document). Cet écrit n'engage toutefois que ses rapporteurs, à savoir le think tank Renaissance Numérique.

TABLE DES MATIÈRES

INTRODUCTION

Jennyfer Chrétien

Déléguée générale de Renaissance Numérique

Renaissance Numérique a toujours porté une grande attention à l'équilibre de nos libertés et droits fondamentaux dans une société qui se numérise de plus en plus. L'irruption dans le débat public des technologies de reconnaissance faciale et de certains types d'usages, nous invite aujourd'hui à nous saisir de ce débat. Nous remercions chaleureusement Monsieur le député Jean-Michel Mis, son équipe, ainsi que la présidence de l'Assemblée nationale pour cette collaboration et cette opportunité de discussion. Il nous tenait réciproquement à cœur d'avoir ce temps d'échange avec l'ensemble des parties prenantes qui portent aujourd'hui une position sur la reconnaissance faciale dans le débat public.

La mise en œuvre des technologies de reconnaissance faciale n'est pas neutre pour notre société. Les décisions qui seront prises sur son déploiement relèveront donc d'un choix politique et d'une vision de notre société demain. Renaissance Numérique en appelle ainsi à ne pas précipiter la réflexion et à prendre le temps de la concertation.

Le think tank a décidé de s'engager lui-même dans cette réflexion et a lancé un groupe de travail, qui réunit une dizaine de ses experts, dont certains interviennent cet après-midi. Nous avons entamé plusieurs travaux afin d'explorer les enjeux de ces technologies, qu'ils soient techniques, juridiques ou géopolitiques ; dont une enquête qui sera présentée dans ce colloque. L'ensemble de ces réflexions donneront lieu à une position et des recommandations que nous présenterons au printemps 2020.

Cette contribution, et celles qui viendront s'adjoindre d'autres acteurs, ne pourront toutefois faire l'impasse d'une véritable concertation, éclairée, avec les citoyens. Ce colloque n'est donc que le début d'une discussion approfondie.

Jean-Michel Mis

Député de la Loire

Je tiens à remercier Monsieur Richard Ferrand, Président de l'Assemblée nationale, qui a souhaité mettre ce colloque sous son haut patronage, ainsi que le think tank Renaissance Numérique pour son engagement et son implication dans l'organisation de ce colloque, et l'ensemble de mes collègues parlementaires pour leur contribution. Je remercie également le Conseil National du Numérique et plusieurs associations comme La Quadrature du Net, et l'ensemble des industriels présents aujourd'hui.

Cet évènement a pour but d'ouvrir la parole sur une technologie sujette à des opinions diverses et à la frontière de plusieurs problématiques : si les expérimentations de son utilisation visent à satisfaire une problématique de sécurité, la technologie de reconnaissance faciale ne saurait être mise en œuvre en portant atteinte aux droits fondamentaux des citoyens, et notamment la liberté d'aller et venir et le droit à l'anonymat.

Certains types d'usages de la reconnaissance faciale s'invitent dans le débat public : son utilisation lors du dernier Carnaval de Nice, sa potentielle future utilisation pour les grands évènements sportifs internationaux tels que la Coupe du monde de rugby en 2023 ou les JO en 2024, ou encore l'application « Alicem », projet de l'État pour permettre de se connecter aux services publics. Puisque la technologie de la reconnaissance faciale porte un enjeu de libertés fondamentales, il était essentiel de prendre en considération la perception de nos concitoyens sur celle-ci. Je salue la présence de l'Ifop qui apportera un éclairage important grâce à l'enquête conduite avec Renaissance Numérique.

Sur ce sujet technologique et de citoyenneté, l'Assemblée nationale doit répondre à des injonctions paradoxales : garantir l'intérêt général de sécurité, garantir à nos entreprises la possibilité de pouvoir travailler sur ces sujets de rupture technologique et pouvoir être des leaders dans leurs domaines en France et à l'international, mais également respecter les libertés individuelles. Il nous faut en tant que parlementaires poser un regard éclairé sur ces questions, lever les doutes sur ce que cette technologie permet ou ne permet pas, mais aussi envisager cette technologie au regard d'autres engagements internationaux de la France comme sur l'intelligence artificielle ou le règlement général sur la protection des données.

Salwa Toko

Présidente du Conseil National du Numérique

Il est sain que nous soyons tous réunis pour parler d'un sujet très complexe : la reconnaissance faciale, qui suscite beaucoup de questionnements. Il provoque également de nombreuses interrogations au sein de l'instance que je préside, dans le monde politique et dans la société civile.

Je vais essayer de donner quelques définitions de la reconnaissance faciale. Au prime abord, c'est une technologie d'identification et d'authentification biométrique, comme les empreintes ou l'iris. C'est un taux de correspondance entre deux gabarits : le premier, que la machine produit à la suite de la capture de notre portrait, et cela quelles que soient les conditions de prise de vue, et le second par la donnée que la machine connaît déjà. Cette technologie est sensible car elle se base sur nos données biométriques, qui sont déjà réglementées. Elle peut de plus être opérée à distance, sans interaction et sans que l'individu soit au fait que son visage est analysé par un algorithme de reconnaissance faciale. Progressivement, cette reconnaissance devient usuelle : pour déverrouiller son téléphone, pour passer des contrôles aux frontières avec son passeport biométrique, pour trier des photos, pour accéder à un lieu ou un outil de travail. La facilitation des parcours des utilisateurs d'authentification ou d'identification, ainsi que la multiplication des capteurs et des sources d'image entrainent la démocratisation de cette pratique.

Pour autant, cette technologie suscite beaucoup d'inquiétudes de la part des citoyens et des experts. En effet, elle porte encore de multiples risques aux fortes conséquences sur les vies humaines, avec des répercussions réelles sur les droits et libertés des citoyens. D'abord le droit à l'égalité, car la technologie est porteuse de nombreux biais, qui sont source de discriminations et qu'il est nécessaire de prendre en considération. Par exemple, cette dernière n'est pas encore fiable pour l'identification de l'ensemble de la population : les taux de reconnaissance des femmes de couleur noire sont extrêmement bas, j'en ai fait l'expérience. Ensuite, le droit à la sécurité, car le caractère particulier des données biométriques, immuable, questionne sur la proportionnalité de leurs usages vis-à-vis des risques de sécurité auxquels ils sont associés. Sommes-nous prêts, technologiquement, à assurer le risque zéro au citoyen pour ses données qui constituent leur individualité ? Enfin, le droit à la vie privée, pour lequel nous nous sommes beaucoup battus, jusqu'à présent avec le règlement général sur la protection des données face aux dérives commerciales ou sécuritaires comme on peut le voir dans certains pays (je ne citerai pas la Chine). Dans ce contexte, que devient la liberté d'aller et venir anonymement ?

Il convient de s'interroger tant sur les technologies, que sur l'acculturation et la formation des opérateurs et créateurs de systèmes : sommes-nous prêts à valider cette technologie qui pourrait mettre en péril notre démocratie et créer des citoyens de second rang dans des espaces de circulation libre, une somatisation de cette possibilité d'identification à tout moment dans tout endroit sans en avoir connaissance ? Comment savoir si nous voulons supporter ce risque ? En rendant les différents acteurs responsables ? En réglementant en fonction des finalités ? Ce sont les questions qu'il faut aujourd'hui se poser, et pas uniquement en tant qu'experts. Face à ces enjeux, beaucoup de voix se lèvent partout dans le monde, pour en parler, pour s'y opposer,

pour réglementer, sur-réglementer, sous-réglementer, pour demander des moratoires en attendant d'avoir des technologies plus fiables et un cadre réglementaire plus précis et strict.

Les échanges sur la reconnaissance faciale et son cadre réglementaire doivent être pensés dans un monde globalisé, avec une vision multilatérale et ouverte au dialogue. La société civile, les usagers, les citoyens ne sont presque jamais dans la salle. Une position franco-centrée ne nous aidera pas à faire évoluer le débat tout en maintenant notre souveraineté. Il faut voir plus grand et travailler à l'échelon européen pour supporter les discussions et les échanges avec des industriels souvent d'échelle internationale. Avec l'Europe, nous pouvons trouver des points d'équilibre, nous pouvons être porteurs de normes dans la transposition de nos valeurs, dans des cadres qui nous ressemblent. Nous devons penser les garde-fous, les lignes rouges à ne pas franchir.

Aussi, j'aimerais saisir l'opportunité de ce colloque à l'Assemblée nationale pour rappeler quelles sont les premières positions du Conseil National du Numérique. Nous considérons et mettrons toujours en priorité le respect des principes du consentement, de frugalité des données, de proportionnalité et d'anticipation des risques. Le CNNum maintient les positions qui ont émergé lors des précédentes mandatures - notamment vis-à-vis du fichier TES - contre la centralisation des données. Le CNNum est contre l'utilisation massive de la reconnaissance faciale, la surveillance généralisée sans limitation de temps et d'espace. Enfin, nous sommes contre l'utilisation de la reconnaissance faciale sur les mineurs.

Pour conclure, un grand nombre d'articles, scientifiques ou non, ont été produits ces derniers mois au sujet de la reconnaissance faciale. Au Conseil National du Numérique, nous avons entamé des travaux qui ont porté un peu à controverse. Nous les poursuivrons et nous rendrons un avis au cours du premier semestre 2020. Les impacts potentiels de la reconnaissance faciale m'entraînent à penser qu'il ne faut pas en faire un débat de niche, que les juristes et les scientifiques ne peuvent pas mener de front seuls ces questions. Merci encore à Monsieur le député Jean-Michel Mis d'avoir ouvert l'Assemblée nationale à ce débat qui est essentiel. Il est essentiel que les citoyens s'emparent de ce débat. Merci de le faire, par le relais des élus. Il faut continuer le travail d'acculturation en étant attentif à placer l'humain au centre, pour permettre à chacun de s'interroger ouvertement, sans exclure l'éventualité d'un rejet global ou d'une acceptation soumise à certaines restrictions.

TABLE RONDE 1 - RECONNAISSANCE FACIALE : USAGES INDUSTRIELS ET COMMERCIAUX

OBJET DE LA TABLE RONDE

Payer, déverrouiller notre terminal numérique, accéder à une zone protégée sur son lieu de travail, vieillir son visage, fluidifier les files d'attente… de nombreuses applications utilisent aujourd'hui des technologies de reconnaissance faciale afin de sécuriser et proposer de nouveaux services. Encadrés par le règlement général sur la protection des données, ces usages plus ou moins sensibles font naître des inquiétudes parmi leurs utilisateurs quant au respect de leur vie privée et à l'exploitation de ces données.

Questions couvertes : Que peuvent faire les entreprises privées avec nos données visage ? Quels usages se développent aujourd'hui sur les lieux de travail ? Quelles protections pour les consommateurs / usagers / citoyens ? Reconnaissance faciale ou visuelle : quelles précautions ? La performance des systèmes actuels n'est-elle pas un obstacle à la multiplication de ces usages ? Biais, transparence et performance : comment ces aspects sont-ils aujourd'hui pris en compte ?

Les intervenants :

- Didier Baichère, Député des Yvelines,
- Vincent Bouatou, Directeur de l'Innovation Lab d'IDEMIA,
- Annabelle Richard, Avocate associée chez Pinsent Masons,
- Mathieu Rondel, Directeur expertise et performance opérationnelle à la Direction des Opérations Aéroportuaires du Groupe ADP.

Vincent Bouatou

Directeur de l'Innovation Lab d'IDEMIA

IDEMIA est un fournisseur de technologies et de solutions de sécurité, ce qui inclut les technologies de reconnaissance faciale. Nous sommes basés en France, notre R&D consacrée à la reconnaissance faciale est installée en France et en Allemagne. Nos cas d'usage dans le domaine gouvernemental ont été évoqués : le passage aux frontières automatisé ; l'identité numérique, c'est-à-dire la capacité à établir une identité en ligne de manière sûre ; les investigations post-événement par reconnaissance faciale et analyse vidéo au sens large.

Dans le domaine privé, nous fournissons des solutions de mise en relation initiale qui vont permettre à un consommateur d'ouvrir un compte bancaire ou une ligne téléphonique sur internet, en prouvant son identité de manière forte comme la réglementation l'exige pour les opérateurs bancaires et téléphoniques. L'économie du partage est aussi consommatrice de ces technologies : il s'agit de mettre en contact des personnes qui doivent se prouver leur identité avant la mise en relation. Nous vendons également des solutions de contrôle d'accès physique sur le lieu de travail ou d'accès à des zones sensibles. Par exemple, nous avons réalisé un projet à l'aéroport international de Singapour : avec les autorités aéroportuaires, nous avons déployé un parcours utilisateur complet depuis l'arrivée à l'aéroport jusqu'à l'embarquement dans l'avion. L'usage de techniques biométriques, parmi lesquelles la reconnaissance faciale, permet de fluidifier le parcours passager. Le paiement biométrique fait également partie de nos applications.

Nous sommes convaincus que les cas d'application de la reconnaissance faciale où la valeur d'usage ou de sécurité est créée pour l'utilisateur ou l'organisation peuvent se déployer dans le cadre légal, avec la volonté de protection des données personnelles et de la vie privée qui est très importante. À ce sujet, il nous semble que l'expérimentation est un élément important dans une stratégie pour aller de l'avant sur ces sujets. Cela permettra de démystifier de manière probante les capacités et les vulnérabilités de cette technologie, de mettre en évidence (ou non) la valeur d'usage créée, de faire un exercice de transparence qui servira d'exemple à de futurs déploiements et sous quelles conditions. Il nous semble important que la France et l'Europe se dotent d'organismes indépendants capables de faire l'évaluation de ce genre de technologies, car aujourd'hui cela manque cruellement à l'échelle européenne. Il nous semble naturel qu'un débat ait lieu sur le sujet du déploiement et nous envisageons naturellement d'en faire partie.

Annabelle Richard

Avocate associée chez Pinsent Masons

Le cadre réglementaire n'est pas inexistant contrairement à ce que l'on peut entendre parfois. Il n'y a certes pas de texte spécifique sur la reconnaissance faciale, mais il y a un cadre générique qui s'applique. D'un point de vue juridique, les technologies de reconnaissance faciale constituent des technologies de biométrie.

La biométrie correspond à l'ensemble des technologies qui, par un ensemble de procédés automatisés, permet de reconnaître un individu à partir de la quantification de ses caractéristiques physiques, physiologiques, ou comportementales. L'élément essentiel de cette technologie est que l'on ne peut

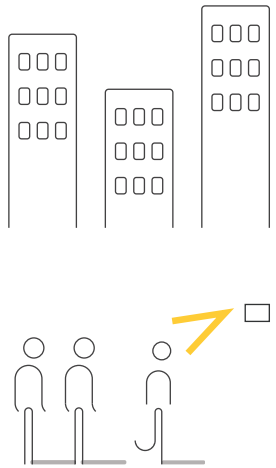
pas se détacher de ces caractéristiques contrairement, par exemple, à un identifiant. Il n'est pas possible de modifier ses empreintes digitales, son iris ou son visage. A cet égard, la technologie exploite les points du visage qui ne peuvent être modifiés, même par la chirurgie esthétique, contrairement à ce que certains mythes véhiculent.

En tant que telle, la reconnaissance faciale est réglementée et incluse dans certains cadres réglementaires depuis longtemps, et a toujours suscité une forme de méfiance. Par exemple, il y a en France cinq textes qui autorisent expressément le recours à la reconnaissance faciale, notamment le fichier de traitement des antécédents judiciaires (TAJ), PARAFE, Alicem et deux autres expérimentations. À l'inverse, vingt-cinq textes qui autorisent des traitements comportant le traitement d'image numérisée excluent ou interdisent expressément l'utilisation de la reconnaissance faciale.

En ce qui concerne le cadre général qui s'applique à la reconnaissance faciale pour les usages publics, il s'agit du cadre réglementaire relatif au traitement des données à caractère personnel, donc la loi de 1978 dite «Informatique et Libertés» et toutes ses évolutions jusqu'en 2016 et l'adoption du règlement général sur la protection des données (RGPD) qui est entré en vigueur en 2018. Avant l'entrée en vigueur du RGPD, les données biométriques n'étaient pas des données sensibles, elles relevaient du régime de demande d'autorisation préalable auprès de la Commission nationale de l'Informatique et des Libertés (CNIL), et dans ce cadre cette autorité a rendu un certain nombre de délibérations. Avec le RGPD, le régime a évolué : la demande d'autorisation préalable a largement disparu, les données biométriques constituent désormais des données sensibles et cela modifie profondément la donne. En effet, en vertu de l'article 9 du RGPD, le traitement des données sensibles est en principe interdit et n'est possible que par exception. Ces exceptions sont diverses, par exemple, le consentement, les cas où cela relève de la sauvegarde des intérêts vitaux, lorsque des motifs d'intérêt public importants l'exigent, ou encore à des fins de recherche scientifique. Notons que cet article 9 laisse une certaine flexibilité aux États membres et leur a ménagé la possibilité d'adopter des textes spécifiques qui viendraient rendre applicables dans chaque État membre les différentes exceptions.

Le RGPD n'a donc pas tout nivelé. D'un État membre à l'autre, il peut y avoir des différences significatives en particulier dans le domaine de la recherche. En France, ce n'est envisageable qu'à certaines conditions et seulement à des fins de recherche publique. Il y a plus d'incertitude concernant la recherche privée. La loi Informatique et Libertés telle que modifiée renvoie bien à l'article 9 et à ses exceptions, mais n'est pas explicite concernant la recherche privée. Cette incertitude est sans doute handicapante pour les acteurs privés.

Comme nous ne sommes plus dans un système d'autorisation préalable, nous nous retrouvons dans un système de responsabilisation des entreprises : chacune doit évaluer son action dans le cadre de la loi et réaliser une analyse d'impact. Sur ce point, la CNIL a établi une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données (AIPD) est obligatoire et cela recouvre notamment les traitements visant à identifier une personne physique de manière unique parmi lesquelles figurent des personnes dites « vulnérables ». D'autres critères issus des lignes directrices du groupe de l'article 29 sont également susceptibles de s'appliquer à la reconnaissance faciale. L'AIPD, c'est la mise en balance de l'atteinte portée aux libertés civiles et aux droits des individus, avec la nécessité de réaliser ces traitements et les mesures de sécurité particulières mises en œuvre pour équilibrer la balance entre risques, réalité et intérêts. Dans le cas où à l'issue de l'AIPD les risques résiduels demeurent significatifs, vous avez l'obligation de transmettre les résultats à la CNIL.



Mathieu Rondel

Directeur expertise et performance opérationnelle à la Direction des Opérations Aéroportuaires du Groupe ADP

Au sein du Groupe ADP, l'expérimentation que nous allons mener début 2020 portera sur la facilitation du parcours passager et non sur la sécurité publique. Notre enjeu majeur porte sur l'amélioration de la performance opérationnelle, notamment la simplicité et la fluidité du parcours pour le passager (et donc la réduction des files d'attente). En arrivant dans une aérogare, un passager doit présenter à plusieurs reprises sa carte d'embarquement et/ou son document d'identité : au moment de l'enregistrement, au dépôt des bagages (il y a une obligation de rapprocher à ce moment-là carte d'embarquement et pièce d'identité), au passage de la sûreté, au passage de la police dans le cas d'un vol international, au moment de l'embarquement (nouveau rapprochement documentaire). Tous ces jalons peuvent générer des points de blocage, avec parfois des temps d'attente qui peuvent être importants.

En parallèle, nous devons faire face à une augmentation de trafic : le Groupe ADP prévoit en effet + 2,6 %/an de trafic sur la période 2021-2025 pour les aéroports parisiens. L'automatisation de nos processus est donc l'un des leviers que nous souhaitons expérimenter pour répondre à l'enjeu capacitaire des années à venir. Nous cherchons à ce que le gain de temps soit significatif sur chaque processus, afin de fluidifier chaque jalon. L'usage de la biométrie, et en particulier de la reconnaissance faciale peut permettre d'optimiser ces étapes automatisées en améliorant la performance opérationnelle sans dégrader la sûreté des processus existants.

Notre parcours vers la biométrie s'est fait progressivement. Les premiers sas PARAFE (Passage Automatisé Rapide des Frontières Extérieures) avec biométrie à reconnaissance digitale ont été inaugurés dans les aéroports parisiens en octobre 2009. Le Groupe ADP a depuis progressivement accéléré leur déploiement et, en juin 2018, un tournant s'est opéré avec le déploiement de la reconnaissance faciale sur ces sas PARAFE. Nous disposions fin décembre 2019 de 102 sas, ce chiffre sera porté à près de 117 au printemps prochain. Le temps moyen de passage aux sas PARAFE est réduit grâce à la reconnaissance faciale : 10 à 15 secondes contre 30 secondes avec la reconnaissance digitale. 45 % de nos passagers sont dorénavant éligibles (majeurs issus de 32 pays : les 28 pays de l'Union européenne et la Suisse, l'Islande, le Lichtenstein et la Norvège), lorsque 10 % de nos passagers étaient éligibles avec la reconnaissance digitale (majeurs issus de 4 pays : la France, la Belgique, le Luxembourg, l'Allemagne).

Par ailleurs, nous avons réalisé une expérimentation avec Air France pour adresser le point spécifique du rapprochement documentaire à l'enregistrement des bagages et à l'embarquement. C'est une étape clé du parcours passager, il est compliqué de mobiliser des personnes dédiées à cette tâche. L'expérimentation consistait à encoder le gabarit du visage du passager et à l'insérer dans le code-barres de la carte d'embarquement. Le voyageur transportait ainsi lui-même le document qui contenait son gabarit biométrique, ici son visage, durant tout son parcours (donc pas de question liée au stockage des données). Le rapprochement documentaire était réalisé au même moment que l'encodage du gabarit du visage, par comparaison entre le nom de la carte d'embarquement et la pièce d'identité que le passager devait présenter. Cette expérimentation a porté sur quelques milliers de passagers et a bien fonctionné. Air France travaille à industrialiser ce processus prometteur, cela nécessite encore des développements informatiques.

Enfin, nous travaillons maintenant sur une expérimentation qui permettra de passer les étapes de l'enregistrement bagages et de l'embarquement avec la simple présentation du visage du passager : plus de carte d'embarquement ou de pièce d'identité à présenter, le visage suffit à franchir chacune des étapes. L'idée générale est la même que précédemment : le passager s'enregistre sur une borne, mais cette fois le gabarit biométrique ainsi que les données de la carte d'embarquement sont stockés temporairement sur une base centrale. Des caméras sur les équipements en enregistrement bagages et embarquement permettront d'autoriser par la simple présentation du visage du passager l'accès au service. Nous travaillons sur cette expérimentation avec la CNIL depuis quasiment un an. Nous sommes très engagés dans le respect des libertés, par exemple les données du passager seront supprimées dès que l'avion décolle. Les données recueillies sont uniquement utilisées pour les fins de facilitation liées à l'expérimentation. Cette expérimentation débutera en mars 2020, et s'étendra sur une année. Nous sommes conscients qu'un stockage de données biométriques sur une base est un sujet délicat. Nous avons eu l'autorisation de la CNIL pour cette expérimentation. En cas de succès et de déploiement plus large, de nouveaux échanges auront lieu avec la Commission. Nous avons bien entendu fourni des gages de sécurité, en termes d'architecture technique, avec des bases séparées, le stockage des gabarits séparé du stockage des informations d'identité, des clés de cryptage entre les différentes bases, etc.

Le Groupe ADP est fermement engagé et considère comme sujet prioritaire le respect des libertés et la stricte conformité aux règles relatives au traitement des données. Nous travaillons main dans la main avec la CNIL, de façon proactive.

Didier Baichère

Député des Yvelines

La réflexion sur la reconnaissance faciale à l'Assemblée nationale n'est pas née de l'engouement du moment. Ce qui m'intéresse à l'Office parlementaire d'évaluation des choix scientifiques et technologiques (qui ne traite pas que de sujets purement scientifiques au sens techniques), c'est la question de l'usage, quand on dépasse une forme de rationalité. La forte notoriété de la reconnaissance faciale, comme le montre le sondage que vous avez réalisés avec l'Ifop, est directement liée aux usages quotidiens que les industriels proposent et que nous avons adoptés. L'usage doit-il s'imposer ou bien faut-il remettre de la rationalité ? J'avais effectué le même travail sur les objets connectés, il y avait d'ailleurs la même irrationalité que pour la reconnaissance faciale.

J'ai produit un rapport parlementaire qui présente des alertes et des recommandations, notamment sur une méthodologie que nous cherchons à partager. Pour les alertes, je n'ai pas trouvé d'éléments probants durant les quatre mois d'audition qui ont montré que la technologie était infaillible. Autre alerte : les élus des collectivités locales, qui font preuve d'une profonde méconnaissance, et d'une manipulation du sujet à travers la vidéoprotection que j'estime très légère, en tout cas qui ne va pas au fond du sujet selon moi. J'estime qu'il aurait fallu approfondir la formation et le dialogue avec les citoyens des communes avant d'arriver à la situation d'installation sécuritaire de vidéoprotection actuelle. Dans certaines communes, les citoyens n'ont aucune idée de ce qui se passe réellement : on a créé une illusion de sécurité. Ce que l'on pratique aujourd'hui avec la vidéoprotection est vraiment dangereux, peut-être davantage que la reconnaissance faciale. Troisième alerte : l'absence de formation à l'économie de la donnée. Quand un usage est constaté *ad hoc*, il faut l'accompagner de savoirs. Par exemple, un adolescent qui s'inscrit sur Facebook ou déverrouille un smartphone n'a pas conscience à ce moment-là de nourrir un système économique avec des données gratuites au profit d'autres personnes. C'est un sujet qu'il faudra aborder avec l'Éducation nationale si l'on veut avoir des citoyens éclairés, afin que chacun puisse mesurer la dimension économique. Évidemment, le cadre légal doit aussi s'assurer du respect des libertés individuelles. Avec ces technologies, le rôle protecteur de l'État est fondamental et doit être réaffirmé avec force.

Pour les recommandations, nous avons mis en avant la transparence et l'éthique. La reconnaissance faciale comme l'intelligence artificielle, devra toujours laisser la décision finale à un humain et non à la machine, et s'assurer que l'on peut toujours auditer ce que l'on est en train de faire, ce qui est souvent complexe quand on entre dans le détail d'algorithmes. Le débat n'est d'ailleurs pas tranché sur l'audit avant ou après. Notre recommandation porte sur deux sujets : expérimenter et consulter. Expérimenter, cela veut dire sortir du cadre actuel, qui est pratiqué par des industriels dans le cadre du RGPD pour des applications commerciales, mais aussi des collectivités locales qui expérimentent de manière peu scientifique. Aujourd'hui, on ne peut pas croiser les données entre les expérimentations, elles restent dans leur coin. Se pose également la question de la souveraineté en précisant qui propose la solution, qui propose l'algorithme. C'est d'ailleurs parfois flou, avec des briques logicielles laissées à disposition d'applications : dans ce cas, qui est l'opérateur responsable ?

L'enjeu est de poser le cadre expérimental : qui, avec quels industriels, dans quel écosystème académique (qui doit être partie prenante de la méthodologie comme du contenu), avec quels organismes de contrôle (il est important que le CNNum et la CNIL suivent ces expérimentations pour s'assurer de la régulation). En parallèle, il faut lancer la consultation effective auprès des citoyens. La notoriété de la reconnaissance faciale est forte, mais il faut faire de la pédagogie. Il existe des cadres dans d'autres domaines qui fonctionnent très bien, par exemple les lois de bioéthique : la loi décrit comment effectuer les consultations en ligne et dans les territoires, comment tirer des citoyens au sort pour qu'ils émettent un avis, quel type de synthèse sera remis à l'Office parlementaire d'évaluation des choix scientifiques et technologiques. Ce rapport de l'OPECST pourra nourrir les futurs débats parlementaires.

L'Europe doit également jouer son rôle : la nouvelle Présidente de la Commission européenne a cité dans son agenda des cent jours la nécessité d'avancer sur l'intelligence artificielle (IA) et sur la reconnaissance faciale, qui est une des premières applications opérationnelles de l'IA. À ce stade, il n'est pas certain que l'Europe puisse et veuille légiférer sur la reconnaissance faciale. En revanche, les différents pays pourraient partager un même cadre méthodologique d'expérimentation et de consultation citoyenne pour avancer au même rythme et adapter ensuite la réglementation à la fin de ces deux ou trois années d'expérimentation.

Nous en sommes là aujourd'hui. Je ne crois pas à l'interdiction de la reconnaissance faciale, et d'ailleurs à quel titre serait-elle prononcée, comment l'État pourrait appliquer une interdiction pour un sujet qui n'est pas scientifiquement ni concrètement maîtrisé ? Je ne crois pas non plus au moratoire sur un sujet pas encore défini ni discuté. La loi française pourra en revanche poser des lignes rouges, évidemment. La France a devant elle des temps forts comme la Coupe du monde de rugby ou les Jeux olympiques. Tous les pays qui connaissent de grandes manifestations en profiteront pour mener des expérimentations. Nous devons tenir compte de ce calendrier, pendant lequel la France aura un rayonnement important et pourra affirmer son soutien à ses champions industriels. Une voix française existe en matière de reconnaissance faciale. Elle n'est pas basée sur des impressions ou des peurs mais bien sur des faits scientifiques, une méthodologie, une expérimentation contrôlée et transparente.

DISCUSSION

Marine Pouyat

Administratrice de Renaissance Numérique et Consultante, experte en protection des données et vie privée (modératrice)

Vous avez tous évoqué l'Europe, car le débat dépasse évidemment la France. Quel est l'état de l'art de la réglementation et de la réflexion dans les autres pays ? La question des bases de données se pose également. Il semble que plus la taille de la base augmente, plus la difficulté à la sécuriser s'accroit également et qu'au contraire s'il y a un stockage en local la sécurité serait mieux maitrisée : est-ce que c'est le cas ?

Annabelle Richard

Avocate associée chez Pinsent Masons

Le RGPD est un texte d'application directe, à vocation européenne. Donc les règles qui s'appliquent en France sont pour l'essentiel les mêmes que celles qui s'appliquent dans les autres pays européens. Les différences sont donc à la marge, parfois liées à des usages spécifiques. Par exemple, le Royaume-Uni est le premier pays à utiliser la reconnaissance faciale à partir de «vraies» bases de données (sans passer par des tests comme à Nice). C'est très particulier puisque le pays est sur le point de quitter l'Union européenne, il a donc pris une certaine « avance » qu'il compte garder. La reconnaissance faciale a ainsi été déployée au Royaume-Uni au cours de grands événements, comme la finale de la Ligue des Champions UEFA 2017, certains matchs de rugby, ou encore des concerts. Ce sont des déploiements réels, pas avec des personnes volontaires. Pour l'UEFA en 2017, la reconnaissance faciale a même permis l'identification et l'arrestation d'un individu recherché pour des faits de violence domestique. Ces déploiements ne sont toutefois pas à l'échelle territoriale globale du pays, ni en continu : il s'agit d'événements circonscrits dans le temps et l'espace.

L'Italie s'intéresse beaucoup à la reconnaissance faciale. Les Pays-Bas sont également assez avancés car ils ont déjà fait application de l'exception concernant la recherche prévue à l'article 9 du RGPD ; dans la me-

sure où le traitement est nécessaire à des fins de recherche scientifique, les recherches sont dans l'intérêt public, la demande de consentement explicite s'avère impossible ou implique un effort disproportionné et l'exécution prévoit des garanties telles que la vie privée de la personne concernée ne soit pas affectée de manière disproportionnée.

Hors Europe, tout le monde a entendu parler du cas de la Chine. Le cadre réglementaire n'est d'ailleurs pas tout à fait inexistant : il y a une loi spécifique qui peut s'avérer très handicapante sur les transferts de données entre la Chine et d'autres États. Le pouvoir législatif en Chine se montre souple pour pouvoir adopter les différents usages lorsqu'ils sont voulus. Aux États-Unis, le sujet fait débat et a donné lieu à des décisions récentes. En mars 2019, le *Commercial Facial Recognition Privacy Act* a été présenté au Sénat américain. Il vise à encourager un certain nombre d'usages. Certaines villes comme San Francisco, Oakland ou Berkeley ont prononcé des interdictions d'utilisation des technologies de reconnaissance faciale par les services de police, en particulier par les caméras embarquées sur leurs gilets. La Californie a même adopté un moratoire de trois ans.

Les principales discussions hors de France portent sur deux points importants : la nécessité de faire un pas de côté et de ne pas poser d'abord la question des conditions de mise en œuvre de la technologie de reconnaissance faciale, mais d'abord se demander s'il faut le faire. Quelle est la nécessité de cette technologie au regard des questions qu'elle pose ? La deuxième interrogation est celle de la responsabilisation des acteurs comme l'évoquait Monsieur le Député : on s'interroge souvent sur la responsabilité des fournisseurs de technologie et pas assez sur celle des utilisateurs de la technologie. Ce que la technologie donne, c'est un pourcentage de chances que le gabarit A corresponde au gabarit B, ensuite un individu doit décider si oui ou non c'est un motif suffisant pour intervenir. Cela nécessite donc qu'il en sache assez sur les enjeux pour prendre une décision, mais aussi qu'il sache comment aborder Monsieur ou Madame Untel, parce qu'à ce stade ces personnes ne sont coupables de rien : il y a juste une potentialité de reconnaissance. La manière d'aborder l'individu relève donc de l'utilisateur et c'est crucial.

Mathieu Rondel

Directeur expertise et performance opérationnelle à la Direction des Opérations Aéroportuaires du Groupe ADP

Dans le cas de l'expérimentation de la carte d'embarquement biométrique, la base de données sert à stocker le gabarit du visage et à le comparer à chaque jalon. Cette base ne contient pas de photo préalable, l'algorithme doit effectuer les rapprochements entre items mais la base ne contient que le strict nécessaire pour arriver aux finalités de l'expérimentation.

Pour l'expérimentation, il y a une demande d'accord du passager, de manière très transparente : on l'informe de ce qu'il advient de ses données, il a tout au long du processus le droit de les supprimer sur le champ de la base s'il le désire. Les données ne sont pas utilisées de manière commerciale : on ne croise pas les données avec son profil Facebook pour lui faire des offres ciblées quand il se trouve dans la zone commerciale (*duty free*).

Les principales interrogations sur la base de données portent sur les éventuelles brèches de sécurité. Le risque évidemment, c'est que plus la base contient d'informations, plus il y aura d'informations « en liberté » en cas de brèche, d'où l'importance d'avoir une base complètement sécurisée.

Marine Pouyat

Administratrice de Renaissance Numérique et Consultante, experte en protection des données et vie privée

Évoquons rapidement les biais et la performance.

Vincent Bouatou

Directeur de l'Innovation Lab d'IDEMIA

Concernant les biais, il s'agit d'une hétérogénéité de taux d'erreur selon les populations considérées par un algorithme donné : genre, âge, groupe ethnique... Ces populations peuvent présenter des différences de performance qui sont mesurables. Les efforts à l'échelle internationale et les progrès de l'intelligence artificielle font diminuer les taux d'erreur d'un facteur 2 tous les ans : les progrès réalisés ont vocation à aplanir les taux d'erreur.

Ce sujet nous tient à cœur chez IDEMIA, car il n'est pas question qu'une personne exploite un biais pour frauder un passage à la frontière. Nous sommes attentifs à ce que les taux d'erreurs soient répartis sur la population. C'est un travail scientifique, nous collaborons avec un certain nombre d'académiques, à la fois membres de chaires ou de groupes rassemblant des chercheurs d'entreprises sur ce type de problématiques. Les biais continueront à diminuer de manière mécanique tant que l'on fournira cet effort.

Enfin, les biais sont liés à la représentativité de la population donnée au moment de l'apprentissage des algorithmes. Si une population n'est pas présente dans la base qui a servi à développer l'algorithme, il est mécanique et évident que les performances de l'algorithme sur cette population sera plus faible. Le cœur du sujet, c'est donc bien la représentativité des bases d'apprentissage.

Didier Baichère

Député des Yvelines

Les biais et la performance dépendent très largement des cas d'usages. Premier cas, la gestion de flux, par exemple avec le billet / visage. Deuxième cas, la sécurité avec PARAFE. Troisième cas, le marketing : gros monsieur / grand menu, vieux monsieur / crème antirides... l'analyse morphologique aura un impact sur les suggestions de vente dans un magasin. L'étude de Renaissance Numérique et de l'Ifop montre une faible acceptabilité de ce cas-là. Quatrième cas d'usage que l'on a rajouté et qui est intéressant, par exemple s'assurer que l'on opère bien la bonne personne. Il y a plus de cas d'erreurs qu'on n'imagine. Le vieillissement de la population fait que nous souhaitons vieillir à la maison. Si une personne âgée perd la tête, il est peut-être souhaitable que dans le cadre d'une collectivité, on transmette une photo pour la retrouver et l'identifier. Quand nous avons rencontré le groupe d'experts sur l'intelligence artificielle à la Commission européenne, nous avons soulevé le cas du handicap : certaines situations pourraient être améliorées par la reconnaissance faciale.

Arthur Messaud

Juriste à La Quadrature du Net

À propos du projet de reconnaissance faciale avec ou sans carte, la base légale est bien le consentement, dans les deux cas ? Est-ce que vous allez renforcer la voie d'accès sans biométrie pour réduire la queue ?

Mathieu Rondel

Directeur expertise et performance opérationnelle à la Direction des Opérations Aéroportuaires du Groupe ADP

On demande effectivement le consentement au passager, qui peut choisir les deux options sans être lésé. Pour le moment, il y a trois bornes d'essai donc la question de la différence ne se pose pas, mais c'est un point que nous avons vu avec la CNIL, il doit y avoir une égalité de traitement entre les personnes volontaires et les autres - comme sur PARAFE -.

Corinne Murcia-Judy

Directrice des affaires stratégiques de Surys

Nous sommes spécialistes de l'identité numérique, dans ce cadre il y a un aspect reconnaissance faciale, effectivement soit pour authentifier soit pour identifier, avec ou sans base de données, avec des niveaux de certification différents et des contraintes différentes.

La biométrie n'est pas fiable à 100 % : on peut modifier un visage. Il y a des techniques connues comme le *morphing* qui permettent de frauder, il y a aussi des solutions pour y parer.

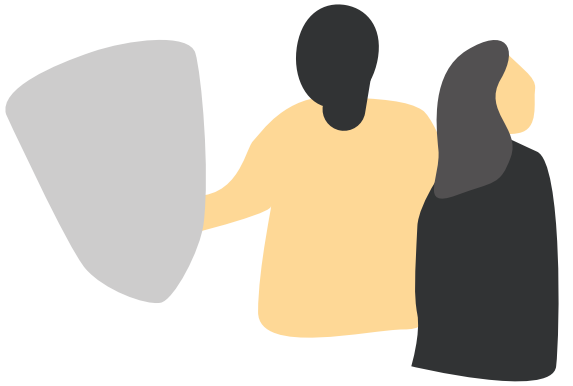
Comment ces expériences, notamment chez Paris Aéroport, s'inscrivent dans le projet français d'identité numérique ? Y a-t'il une cohérence entre ces cas d'usages, expérimentations et études ? Avez-vous défini des niveaux d'authentification différents selon les usages, qu'ils soient privés ou régaliens ?

Didier Baichère

Député des Yvelines

Il serait bon de ne pas demander aux parlementaires de prendre position sur un sujet pour lequel ils n'ont pas les éléments. Nous devons prendre position non pas sur des impressions, mais sur les résultats objectifs d'une expérimentation scientifique et d'une consultation éclairée auprès des citoyens.

TABLE RONDE 2 - RECONNAISSANCE FACIALE ET LIBERTÉS PUBLIQUES : INSTRUMENT DE SÉCURITÉ, TECHNIQUES DE SURVEILLANCE



OBJET DE LA TABLE RONDE

Si le débat de la reconnaissance faciale est aujourd'hui au sommet des agendas politique et médiatique, c'est notamment du fait de l'inquiétude que génère l'utilisation de ces technologies par la puissance publique, laissant apparaître le spectre d'une société de surveillance. Alors que dans le monde, les instances de police et renseignement se félicitent de l'arrivée de ces nouvelles technologies, certaines villes font au contraire le choix d'interdire totalement dans les rues ces usages. Au-delà des finalités de sécurité, tout un pan de nouveaux usages se développent pour permettre l'authentification et l'accès à des services publics, toujours en suscitant de vifs débats.

Questions couvertes : Quels sont les contours de ces innovations menées par les puissances publiques aujourd'hui et leurs différentes finalités ? Biais, transparence, performance, souveraineté : comment intégrer ces enjeux dans les usages de la reconnaissance faciale par la puissance publique ? Y a-t-il une échelle de l'acceptabilité, ou le besoin de rejeter en bloc ces innovations au nom des libertés fondamentales ?

Les intervenants :

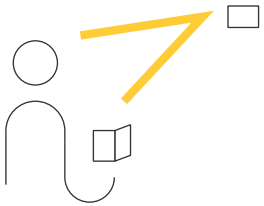
- Raphaël de Cormis, Vice-président Innovation et Transformation numérique de Thalès,
- Étienne Drouard, Avocat associé chez K&L Gates,
- Christine Hennion, Députée des Hauts-de-Seine,
- Dominique Legrand, Président de l'Association Nationale de la Vidéoprotection,
- Alexandre Touzet, Maire de St-Yon.

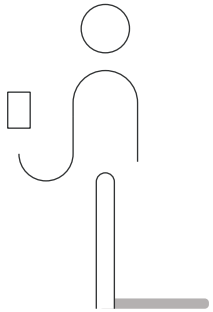
Raphaël de Cormis

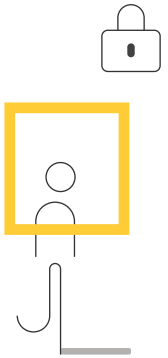
Vice-président Innovation et Transformation numérique de Thalès

Quand on parle de reconnaissance faciale, trois éléments ont un impact sur la performance : l'algorithme, la donnée, et le cas d'usage. Pour des technologies anciennes de trente ans, les algorithmes qui fonctionnent en réseaux de neurones ont des performances qui s'améliorent sans cesse, à la fois dans la vitesse de traitement et dans la précision, et ce afin de réduire le nombre de faux positifs et de faux négatifs. L'enjeu est de régler cette précision selon les cas d'usage, pour éviter de faire rentrer une personne là où elle ne doit pas, et à l'inverse ne pas refuser l'accès à une personne.

À l'heure actuelle, les bases de données publiques que nous utilisons pour les entrainements peuvent impacter les performances des algorithmes sur certaines catégories de populations et nous travaillons à les rééquilibrer. Pour cela, il faut s'assurer que ces données d'entrainement soient correctement labellisées afin que les erreurs ne se répercutent pas. À chaque nouvelle version des algorithmes, nous vérifions qu'il n'y a pas de régression de la performance.







L'ensemble des progrès de la capture, la prise de vue, touche au prétraitement pour améliorer l'image et calculer ensuite sa représentation numérique. Point important, nous remarquons un certain nombre de fraudes possibles et d'usurpation d'identité. L'enjeu de ce qu'on appelle la preuve de vie, qui permet de s'assurer que l'on est bien la personne en chair et en os que l'on prétend être, est clé. Il y a également un sujet de sécurité de la donnée d'entrainement : plus les données sont importantes, plus la taille du pot de miel (*honeypot*) peut attirer des attaquants et mettre à risque des utilisateurs. Autre sujet important : comment utiliser, en situation d'exploitation, la donnée en cas d'erreur ? Dans des cas d'usage physique, il n'est pas possible de récupérer la donnée.

La technologie est neutre en soi, donc tout dépend du cas d'usage. Dans la majorité des cas que nous traitons, qui sont de la fluidification d'expérience physique ou numérique, on n'a pas besoin du visage. Par exemple, pour la mesure d'une foule dans un espace donné, une simple silhouette peut suffire : on traite alors des données anonymes. On a évoqué les choix alternatifs. Nous accompagnons justement nos clients pour mettre en place des solutions alternatives qui accompagnent l'utilisateur dans ses démarches.

Étienne Drouard

Avocat associé chez K&L Gates

Les méthodes d'encadrement juridique sont vieilles mais pas inadaptées pour autant. Pour aborder les sujets de liberté publique, le principe est primordial. En 1980, un rapport d'une vice-présidente de la CNIL « Loi, image et protection des données personnelles » décrivait déjà l'enjeu de la reconnaissance faciale, cela n'a pas pris une ride. La plus mauvaise manière de s'en prendre aux libertés publiques, c'est de s'en remettre au consentement des personnes. Si on est dans le contrat social, ce n'est pas l'individu qui décide, c'est la société, et tout l'enjeu n'est pas « comment » mais « pourquoi ». Il y a deux conséquences à cela : si sur le plan scientifique il y a des approximations, il faut qu'elles soient les plus faibles possible pour protéger les libertés publiques et que l'on se trompe le moins possible. Il faut donc expérimenter la technologie pour augmenter les niveaux de liberté. Si on s'accommode de quelque chose qui peut porter atteintes aux libertés publiques, on protège moins bien l'enjeu d'identification des personnes.

Cela a été dit à plusieurs reprises. Il y a eu un référé devant le Tribunal de grande instance de Paris en 2003 parce que l'on voulait repérer des sil-

houettes afin d'effectuer un comptage publicitaire dans le métro parisien. Une plainte a été déposée pour savoir si cela portait atteinte aux libertés, si cela faisait appel à de la biométrie, si on distinguait une poussette d'un animal, si une personne regardait le panneau publicitaire de face, etc. On avait là les ingrédients d'un usage décomplexé de la technologie qui ne posait problème que s'il y avait méconnaissance de la technique : on ne reconnaissait pas de visages mais la technologie n'était pas recevable socialement.

En France, il y a quarante ans d'histoire sur ce sujet et quelle que soit la modernité de la technique employée, la question sera toujours celle de la proportionnalité. Je suis inquiet que l'on doive légiférer dans le domaine, car la réglementation est déjà tellement complète que l'on ne fera que créer des exceptions. Si on cherche dans le RGPD ou dans la directive Police-Justice une réponse sur la reconnaissance faciale, on va prendre cinq ans dans la vue et ces textes ne sont de toute façon pas faits pour apporter des réponses à ce sujet, ils ne fournissent que la méthode. La méthode, c'est la finalité publique, la proportionnalité, la durée, le type de capteurs utilisés, les données traitées, etc. C'est déjà le travail de régulateurs quotidiens qui existent. Créer une nouvelle loi serait considérer qu'ils ne travaillent pas si bien, ce serait présomptueux.

Les textes existent déjà, alors quel est l'usage que l'on en fait ? Il faut sortir du biais du consentement, qui est le plus mauvais usage. Et plus on sera mauvais, moins on se posera les bonnes questions si on saute à pieds joints dans la volonté d'expérimenter. Pour bien protéger les libertés publiques, je pense qu'il faut qu'on ait une reconnaissance faciale européenne qui ne consiste pas à acheter des gabarits européens à des chinois, des israéliens ou des américains. Nous devons savoir faire pour décider quoi faire et pourquoi, en respectant les questions de finalité et de proportionnalité.

Cela ne se fera que dans une société qui est prête à entendre : on est tous prêts à déverrouiller un téléphone, pas forcément à se faire reconnaître dans un stade pour des motifs de violence conjugale. L'installation de la reconnaissance faciale dans un stade était pour trouver des hooligans, pas un mari violent. La Cour de Cassation a déjà traité des cas de ce genre : peut-on licencier un salarié qui a couché avec la fille du patron sur le comptoir d'un casino, alors que la caméra est là pour vérifier s'il y a des fraudes en caisse quand on échange des jetons contre de l'argent ? Quand on autorise un point de collecte ou de captation des données, il n'y a pas de détournement de finalité à constater autre chose que ce qu'on avait initialement prévu. On ne met pas un œil pudique à la caméra quand on filme pour un objectif précis, ce sera pareil pour la reconnaissance faciale : d'autres usages surviendront. Historiquement, on n'a jamais su résister à la tentation d'un usage secondaire d'une donnée lorsque le point de collecte a été considéré comme légitime. Cet enjeu du détournement de finalité doit être pris en compte, comme il l'a toujours été.

On ne fait pas que des choix pratiques, on fait aussi des choix éthiques et esthétiques : il y a des arbitrages et équilibres à trouver. Plus le débat avance sous un biais technologique, moins on s'autorise à réfléchir avec sérénité sur les libertés publiques. J'ai des craintes quand on parle de lois spéciales : cela crée un problème de temps et un problème d'exceptions.

Dominique Legrand

Président de l'Association Nationale de la Vidéoprotection

J'aimerais d'abord insister sur la CNIL dont on ne parle pas beaucoup. Maître Drouard a rappelé qu'il y a déjà un cadre large, le RGPD est un cadre fantas-

tique qui ouvre des opportunités. Or, je trouve que ces derniers mois, la CNIL s'est comportée en "*sniper*".

Trois exemples. Je découvre abasourdi hier dans ma revue de presse que l'on va demander aux établissements scolaires de réorienter, retirer ou déplacer les caméras de vidéosurveillance pour ne filmer que les espaces de circulation et accès ou les paramétrer pour qu'ils ne fonctionnent qu'en dehors des heures d'ouverture. En résumé, plus de caméra dans la cour d'école, dans les couloirs, etc. Finalement, les caméras sont autorisées du moment qu'on les débranche. Je ne comprends plus. Je ne comprends pas comment la CNIL décide, fonctionne, je ne vois pas de laboratoire (même s'il existe). Ce qui s'est passé à Saint-Etienne est incompréhensible, on jette le bébé avec l'eau du bain. J'ai actuellement deux membres de l'Association Nationale de la Vidéoprotection (AN2V) qui travaillaient sur ces sujets qui n'ont plus de commandes, parce qu'il y a eu un avis de la CNIL repris par l'*AFP*. Une peur s'installe pour les donneurs d'ordres, j'ai plein d'exemples.

Avant de parler de reconnaissance faciale, un simple capteur audio qui détecte une déflagration, un coup de feu, une femme qui hurle, un contact sec est interdit à cause du fantasme de la Stasi. La CNIL dit : on ne voit pas le mot « audio dans les textes, donc c'est interdit ». L'impact c'est une perte d'efficience potentielle des recommandations de la CNIL et des dépôts de bilans. Quels sont les critères pour frapper si fort ? À l'opposé, la caméra de vidéosurveillance d'Amazon fait frémir, elle est ouverte, on peut tout filmer… mais tout va bien. J'aimerais que les énergies se réorientent là où cela fait mal - GAFA, BATX - et que l'on arrête d'embêter les personnes là où elles travaillent de manière éthique avec des organes de contrôle.

Plus personne n'ose rien déployer, y compris un contact audio ou une caméra. Ne cherchons pas à rajouter une couche légale alors qu'il existe déjà un cadre. Dans certains cas, la reconnaissance faciale serait très utile, on s'oblige à faire un *tracking* non biométrique alors qu'il serait plus simple et plus efficace de s'appuyer sur une photo. Je pense au cas de la SNCF : un individu a donné un coup de couteau à une personne, pas de liberté pour lui. La CNIL est incompréhensible dans ses choix et sanctions. C'est pourquoi j'ai un fort doute sur le déploiement de la reconnaissance faciale, mais je demande à être rassuré. À l'AN2V, nous avons identifié des propositions gratuites pour l'État (propositions 6, 12 et 36 du rapport Thourot-Fauvergue) qui libèrent les énergies et augmentent l'efficience des forces de l'ordre. Qu'est-ce que l'on attend ?

Une représentante de la Commission nationale de l'Informatique et des Libertés

Concernant les lycées, la CNIL a fait une mise en demeure à la suite de vingt-cinq plaintes reçues : y filmer de manière continue est un usage excessif et disproportionné.

Alexandre Touzet

Maire de St-Yon

La doctrine de l'Association des Maires de France sur la reconnaissance faciale n'est pas à ce stade définitivement fixée. Nous nous appuyons sur le principe de légalité et le principe de liberté. Il faut partir d'un diagnostic local pour arriver à une solution de sécurité opérationnelle.

Je suis Vice-Président d'un conseil départemental et j'ai en charge la vidéoprotection. Nous commençons par un diagnostic de sécurité avant de mettre en place la vidéoprotection, justement pour respecter le principe de proportionnalité. Les collectivités locales sont mobilisées sur la sécurité, mais avec en toile de fond un progrès scientifique important et un cadre légal qui nous semble assez incertain. Nous avons besoin de clarification, de logiques de rescrit, et d'une législation stabilisée. Par essence, notre travail pourra faire l'objet de contestation du citoyen, la sécurité juridique de l'acteur local est donc indispensable.

Des collectivités ressentent un besoin d'expérimentation, à la fois sur l'authentification et l'identification, avec une pluralité d'objectifs. Il convient d'appliquer le principe de proportionnalité, mais aussi être en capacité de monter en puissance, soit sur des événements ponctuels (exemple à Lyon pour chercher un terroriste), soit sur des événements conjoncturels de renforcement de mesures de sécurité, par exemple face à une menace terroriste renforcée. L'expérimentation, sous le contrôle de l'État, facilitera l'adaptation aux circonstances, la péréquation entre les territoires et la maîtrise des coûts.

L'acceptation sociale de la reconnaissance faciale, et de tous les dispositifs de sécurité en général, est compliquée à établir. Elle est évolutive selon les époques et les circonstances. Il y a une vingtaine d'années, j'avais élaboré le contrat intercommunal de prévention de la délinquance. Quand je parlais de sécurité dans les collèges, il y avait souvent une forme d'incompréhension. Aujourd'hui, je déploie de la vidéoprotection sur une centaine de collèges et je n'ai pas de retour négatif de la communauté enseignante. Il y a dix ans, c'était un sujet de débat, c'était une ligne de partage politique. L'acceptabilité sociale et politique évolue très rapidement selon les circonstances, selon les publics.

Il y a des outils de concertation avec les conseils locaux et intercommunaux de prévention de la délinquance qui réunissent l'ensemble des acteurs : police, gendarmerie, bailleurs sociaux, transporteurs. On peut réfléchir collectivement au bon niveau de sécurité à mettre en place, dans un dialogue entre corps intermédiaires, qui peut être conforté dans un dialogue citoyen. C'est aussi la bonne échelle pour réfléchir à un éventuel rehaussement des dispositifs, autant que de besoin.

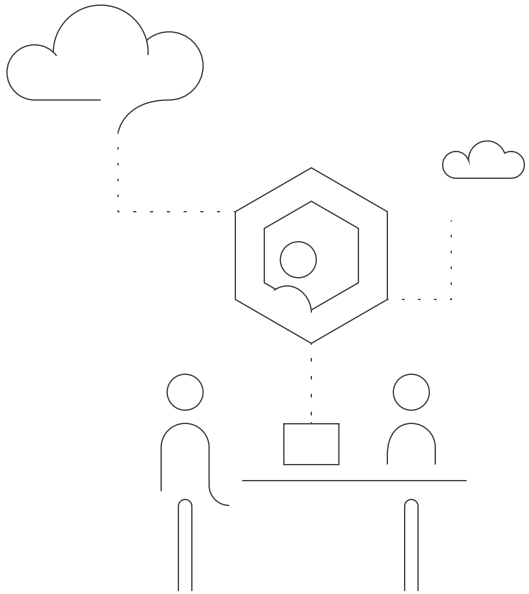
Christine Hennion

Députée des Hauts-de-Seine

J'ai été avec ma collègue Albane Gaillot, une des rapporteurs sur le RGPD. Avec Paula Forteza, nous avons été missionnées par l'Assemblée nationale pour faire un rapport sur l'identité numérique, dans l'objectif de la carte nationale d'identité électronique, applicable en France à partir de l'été 2021. C'est un sujet que nous n'abordons pas par le prisme de la reconnaissance faciale, car ce ne serait pas la bonne finalité. Je pense qu'il faut différencier l'identité numérique des technologies, comprendre les finalités au niveau régalien, comment les transcrire dans un monde numérique, les avantages que l'on peut en retirer. Je suis à la commission des affaires économiques de l'Assemblée nationale, et c'est dans ce cadre que je me penche donc sur les usages que les citoyens pourront en tirer : par exemple, on utilise FranceConnect pour se connecter aux impôts, à la sécurité sociale, etc.

On a déjà plusieurs niveaux d'authentification et d'identification numériques. Au niveau le plus élevé, on doit s'assurer que la personne existe bien et qu'il n'y pas d'usurpation, c'est pourquoi il faut à un moment donné un tiers de confiance. Il faut évidemment s'interroger sur les finalités, à l'aune de la confiance des différents acteurs. La reconnaissance faciale soulève des questions légitimes : que fait l'État de ces données ? Quelles sont les dérives potentielles ? Le contrôle citoyen est indispensable. La CNIL, dont il faut reconnaître le travail, a peut-être besoin d'autres acteurs pour le contrôle des procédures.

Il faut augmenter la connaissance du citoyen : conserver des données locales sur le citoyen ou tout migrer dans un *cloud* qu'on ne maîtrise pas est totalement différent. Confier des données à une société américaine ou chinoise, ce n'est pas pareil que les confier à un acteur européen ou français. Ces questions sont donc d'ordre citoyennes, d'organisation et d'architecture, mais aussi culturelles. Vous l'avez dit, en trente ans, les appréhensions sont devenues bien moindres. Pour autant, il faut continuer à s'interroger sur la nécessité de la captation des données biométriques.



Marine Pouyat

Administratrice de Renaissance Numérique et Consultante, experte en protection des données et vie privée

Une des questions essentielles est la confiance. Mettons cela en perspective avec l'enquête conduite par Renaissance Numérique et l'Ifop. Est-ce que la technologie fonctionne et produit un résultat fiable ? Est-ce que les citoyens ont confiance ? Comment peut-on pallier les biais technologiques et humains pour s'assurer de la qualité des données d'entrainement ? Comment l'humain est-il formé à interpréter un chiffre de probabilité ? Comment traiter le sujet de la souveraineté technologique pour la reconnaissance faciale quand le principal référentiel n'est pas européen à l'heure actuelle ? Comment communique-t-on auprès du citoyen sur ces sujets très techniques ?

Raphaël de Cormis

Vice-président Innovation et Transformation numérique de Thalès

La technologie fournit un score de probabilité entre deux représentations mathématiques d'images, celle de référence et celle qui est capturée. Le système donne un niveau de seuil, l'étape de calibrage est donc très importante. À chaque fois, il doit y avoir une phase de revue par un être humain. Au-delà du seul algorithme, il faut fournir des outils pour lever les cas de doutes. Aujourd'hui, on peut fournir les données qui ont permis à l'IA de prendre telle ou telle décision : un opérateur humain expérimenté pourra vérifier et comprendre pourquoi ce score est atteint. Il n'y a donc pas seulement une réponse binaire et technologique de la machine pour la reconnaissance faciale, l'humain reste présent.

Il n'y a pour l'instant pas de certification. La technologie est en train d'évoluer. Le mètre-étalon aujourd'hui est l'organe de standardisation des technologies américain, qui publie tous les trimestres un rapport d'évaluation des performances et précisions des différents fournisseurs de technologies. C'est utilisé pour les appels d'offres publics : figurer dans ce classement est un critère éliminatoire. La plupart des appels d'offres hors États-Unis se réfère aussi à ce mètre-étalon. L'Europe pourrait donc utilement se doter d'une méthode comparable.

Les organismes privés commencent à certifier le niveau de sécurité du système contre les usurpations d'identité, notamment pour la biométrie et les empreintes digitales. Cela va sans doute s'étendre à la reconnaissance faciale, par exemple autour de la norme FIDO, ou de Visa et MasterCard qui ont leur propre référentiel de certification biométrique.

Alexandre Touzet

Maire de St-Yon

Je n'ai pas de crainte sur la montée en gamme des outils de sécurité dans les collectivités. Il suffit de poser deux préalables : la mutualisation des formations des agents de l'État et des collectivités, et aussi la mutualisation entre collectivités - notamment entre territoires urbains et ruraux -.

La question de l'acceptabilité est complexe, il y a autant d'avis que de citoyens. La concertation a tendance à susciter la participation des très pour et des très contre, en excluant les expressions nuancées et majoritaires. D'où la nécessité de passer par des corps intermédiaires : bailleurs, transporteurs, représentants des établissements, etc. Il y a déjà des instances installées et des mécanismes de consultation dans les communes et intercommunalités à exploiter.

Étienne Drouard

Avocat associé chez K&L Gates

Il y a un enjeu de souveraineté sur les indicateurs qui ne sont ni français ni européens. Les référentiels créent des *soft laws* qui sont très géopolitiques et qui créent des barrières à l'entrée. L'expérimentation doit servir à évaluer ce qui est de qualité et ce qui ne l'est pas. Le meilleur moyen c'est d'établir nos propres normes de qualité par l'expérimentation.

Par ailleurs, il faut garantir la lisibilité : il est difficile de lire entre les lignes d'une délibération de la CNIL, il est difficile pour une entreprise de s'engager dans un projet si elle craint de se faire retoquer. La seule méthode, c'est d'oser, car cela impose d'être professionnel. Pour cela, il faut une lecture de la CNIL compréhensible. Si certains abandonnent par peur de discussions trop longues, la destruction de valeur n'est que le prix de la peur. Plus le régulateur est lisible, plus le prix de la peur diminue. On ne peut avoir de réponse aux questions que si on les pose. Pour le cas des caméras dans les lycées, cela me parait parfaitement normal. Ce qui serait anormal c'est de conclure qu'on ne peut plus mettre de caméras dans les lycées.

Il n'y a plus d'autorisation préalable, il faut donc agir le mieux possible pour que le dossier passe. Il s'est passé plein de choses en six mois en France et on commence à voir se dessiner des lignes de plus en plus précises entre ce que l'on peut et ce que l'on ne peut pas faire. Au regard des incertitudes posées, on avance plutôt assez vite.

Christine Hennion

Députée des Hauts-de-Seine

Au sujet de la normalisation, il y a déjà un plan sur l'intelligence artificielle dans la coopération franco-allemande. C'est un sujet d'industriels, alors allez-y, foncez et nous vous aiderons. Je trouve que les Français sont trop peu présents dans les instances de normalisation à Bruxelles : allez-y, nous avons besoin de vous !

La confiance du citoyen viendra si on lui montre des choses. Cela peut sembler abstrait, il ne faut pas pour autant lui fermer la porte. Dans ma commune, on pratique le vote par machine. Il y a beaucoup de débats à ce sujet, notamment avec l'Agence nationale de la sécurité des systèmes d'information qui estime que ce n'est pas une bonne méthode. À l'occasion des dernières élections, les citoyens qui contrôlent comme il se doit le processus électoral, étaient très suspicieux par rapport à ce procédé. Je les ai invités à voir l'ensemble du processus, ils ont changé d'avis. Ouvrons les portes, expliquons quelles sont les données, ce que l'on en fait.

Yves Le Querrec

Directeur des relations interbancaires de La Banque Postale et Vice-président du Comité français d'organisation et de normalisation bancaires

Il y a bien des commissions de normalisation internationales indépendantes du National Institute of Standards and Technology (NIST), qui travaillent tout de même avec lui pour établir des standards communs (SC37 du JTC1 sur la biométrie, SC42 du JTC1 sur l'IA). Je travaille avec le Deutsches Institut für Normung (DIN) en Allemagne pour un rapprochement des priorités de normalisation. En février, nous aurons un comité stratégique sur ce sujet de normes, je vous y invite.

Martin Drago

Juriste à La Quadrature du Net

Que pensez-vous d'Alicem, de l'échec du cadre de contrôle comme l'a fait savoir la CNIL ? On a un dispositif de reconnaissance facial validé par le Premier ministre alors que l'autorité de contrôle a dit qu'il n'était pas conforme au RGPD.

Christine Hennion

Députée des Hauts-de-Seine

Pour l'instant, on est au début de la mission et on ne regarde pas que la reconnaissance faciale. Alicem, ce sont des données réconciliées à un moment précis, les données biométriques ne partent pas dans la nature, contrairement à ce qui a été dit dans la presse. La CNIL a certes émis des réserves, elle n'a pour autant pas condamné le système.

Alicem est une expérimentation, personne n'a dit qu'il fallait la déployer partout. Ce ne serait de toute façon pas une solution unique suffisante, car cela supposerait des équipements en téléphones et logiciels qui ne sont pas envisageables aujourd'hui. Il faudra plusieurs technologies en parallèle.

Étienne Drouard

Avocat associé chez K&L Gates

La CNIL a émis un avis, cela ne l'a pas empêchée de faire son travail. Le consentement peut ne pas être conforme au RGPD, et le projet peut aussi aboutir sans qu'il y ait besoin du consentement des personnes : les deux sont possibles. L'erreur a été de tout baser sur le consentement.

Un journaliste indépendant

Il y a près de deux millions de caméras de vidéoprotection en France. Serait-il possible d'y injecter un système de reconnaissance faciale qui analyserait et comparerait avec une base de données comme le fichier des antécédents judiciaires ou celui constitué par Alicem par exemple ?

Étienne Drouard

Avocat associé chez K&L Gates

C'est une question d'argent, beaucoup de ces caméras sont analogiques et ne permettent pas ce type d'opération. La vidéoprotection est peu connectée aux réseaux pour des raisons évidentes. Mais si on devait les relier pour un objectif précis, on n'aurait pas pour autant porté atteinte aux libertés publiques.

Valérie Chavanne

Fondatrice et Avocate chez LegalUP Consulting

On parle de confiance, qui rime avec transparence. Est-ce que les résultats des expérimentations de Thalès ou Paris Aéroport sont partagés ? Quels sont les taux d'erreurs ? En matière de loi, Maître Drouard a raison : il n'est pas nécessaire de rajouter un cadre, il est déjà difficile de se conformer à celui déjà en place, il y a déjà des outils réglementaires. Comment rassurer sur la stabilité juridique ?

Raphaël de Cormis

Vice-président Innovation et Transformation numérique de Thalès

Sur l'amélioration continue pour l'authentification biométrique par exemple d'une connexion à un service bancaire, on peut mettre à jour l'algorithme presque toutes les semaines et on atteint des taux d'erreurs inférieurs à 1 sur 1 million. Un code à 4 chiffres, c'est une chance sur 10 000, donc vous êtes 1000 fois plus sécurisés avec la biométrie.

Valérie Chavanne

Fondatrice et Avocate chez LegalUP Consulting

Faites-vous des recherches pour sortir de la logique d'inflation de la récolte de données pour être meilleurs ?

Raphaël de Cormis

Vice-président Innovation et Transformation numérique de Thalès

Il y a plusieurs sujets. D'abord l'explicabilité : on doit dire aux opérateurs pourquoi on recueille cette donnée. L'autre, c'est la frugalité des données : on ne prend que ce dont on a besoin, avec des règles d'apprentissage mathématiques et symboliques. Enfin, on effectue les calculs au plus près des capteurs pour diminuer le nombre de données sensibles circulant sur les réseaux. C'est d'ailleurs aussi une question de consommation d'énergie.

La reconnaissance faciale hybride utilise des gabarits artificiels, cela limite également le nombre de données biométriques utilisées par l'algorithme.

Étienne Drouard

Avocat associé chez K&L Gates

Comment rassurer ? On paye un conseil. Plus sérieusement, le colloque de ce jour rassemble des personnes de tous horizons et c'est cela la réponse. Il y a un fort enjeu de pédagogie. Le régulateur et le justiciable, qu'il soit citoyen, entreprise ou responsable public, doivent donner des grilles de lecture lisibles. La pensée avance vite quand elle est dans un cadre restreint de quelques experts, elle est plus acceptable et comprise quand elle est plus ouverte.

TABLE RONDE 3 - RECONNAISSANCE FACIALE : GARDE-FOUS ET RÉGULATIONS, QUELLES PERSPECTIVES ?

OBJET DE LA TABLE RONDE

Les deux tables rondes précédentes ont permis de soulever de nombreuses questions, dont une partie trouvera certainement leur réponse dans le cadre de régulations futures. Au vu des risques, quelles réponses peuvent apporter les régulateurs, les législateurs et les entités privées ? La France est loin d'être le seul pays à se poser la question de la régulation de la reconnaissance faciale. Au sein de l'Union européenne et au-delà, les expérimentations et usages se déploient, et les gouvernements et localités prennent des mesures de régulation. Leurs contours sont variés et considèrent les cadres en vigueur : Règlement général sur la protection des données, Directive Police-Justice en Europe et lois nationales.

Questions couvertes : Pourquoi la question de la régulation de la reconnaissance faciale se pose-t-elle aujourd'hui ? De quels cadres s'inspirer, ou au contraire, se détourner ? Quels acteurs pour définir ces nouvelles règles ? Quel cadre international ?

Les intervenants :

- Arthur Messaud, Juriste à La Quadrature du Net,
- John Frank, Vice-président des Affaires publiques Europe de Microsoft,
- Albane Gaillot, Députée du Val-de-Marne,
- Jean Lessi, Secrétaire général de la Commission nationale de l'Informatique et des Libertés,
- Mario Oetheimer, Chef adjoint à l'Unité de recherche et de données de l'Agence des droits fondamentaux de l'Union européenne.

John Frank

Vice-président des Affaires publiques Europe de Microsoft

La technologie peut être à la fois un outil et une arme, tout dépend de comment elle est utilisée. Nous pensons qu'une entreprise qui crée des technologies doit s'assurer qu'elles soient utilisées en tant qu'outils. Nous ne pouvons pas simplement espérer qu'elles soient utilisées à bon escient. Microsoft a été un pionnier de l'intelligence artificielle et de la recherche fondamentale dans ce domaine.

Un de ces projets a des dimensions intellectuelles très intéressantes pour les sciences informatiques, mais ce sont les implications sociales et les usages qui ont des conséquences profondes. Notre conviction profonde est que l'IA doit augmenter les capacités humaines, renforcer et améliorer ce que les humains peuvent faire, pas les remplacer. Les humains peuvent reconnaître les visages. Je ne suis pas bon avec les noms, mais je peux reconnaître un visage. Mais quand on augmente l'échelle, l'IA donne des possibilités. Il y a des cas positifs sur lesquels nous pouvons tous être d'accord, des cas négatifs sur lesquels nous pouvons tous être d'accord, et un entre-deux sur lequel cette salle serait divisée. Et c'est bien, parce que les entreprises de technologies ne devraient pas dicter les règles. Les institutions démocratiques doivent mener la discussion et décider avec les citoyens des règles que la société veut.

On nous demande de faire des choses pour une compagnie, un gouvernement. Ensuite, c'est au consommateur que nous devons en parler. Un principe de bout-en-bout a de nombreuses variables : les caméras utilisées, les circonstances de l'expérience, la qualité des images et de la base de données, etc. Toutes influent sur la réponse à la question. La police nous a sollicités au sujet des caméras embarquées en nous demandant qu'elles puissent inclure un système de reconnaissance en temps réel capable de détecter quelqu'un qui devrait être arrêté. Nous avons dû expliquer que ce système n'était pas assez fiable pour ce type d'application. Ils ne pourraient pas avoir de bons résultats à cause des changements d'exposition à la lumière, du mouvement, etc. Ils risqueraient d'arrêter des gens à tort, et d'avoir un biais vis-à-vis des personnes de couleur. Nous avons dû expliquer cela. L'IA est disponible au sein de nombreuses entreprises, mais toutes ne l'expliquent pas comme nous le faisons. Nous devons créer des obligations de transparence pour les entreprises qui produisent les composants, les briques des systèmes de reconnaissance faciale. Les utilisateurs seront ainsi informés si ceux-ci sont adaptés ou non à leurs usages.

Nous pensons que c'est fondamental pour la sécurité et pour des questions d'efficacité. Quand Paris Aéroport a eu ce processus de réflexion, c'est exactement le type de scénario dont nous devons parler. Nous pouvons avoir des discussions sur l'ajustement à chaque étape. Quand la police veut utiliser des technologies de reconnaissance faciale, il n'y a pas de liste préétablie de ce que chaque partie-prenante a à faire. Établir des bonnes pratiques serait d'une grande utilité dans beaucoup de circonstances.

Il y a eu une décision du tribunal du sud du Pays de Galles qui citait le RGPD, la loi britannique, les bonnes pratiques, les recommandations policières, etc. La cour a statué qu'il y avait suffisamment de garanties pour un bon usage. Il serait très utile de créer des bonnes pratiques applicables au niveau national. Nous avons besoin d'un cadre global, mais également d'un système agile qui saurait s'ajuster aux particularités, alors que la technologie progresse et que les consommateurs s'habituent à certains scénarios ou en rejettent d'autres. Il est intéressant dans l'enquête que l'usage de la reconnaissance faciale pour le déverrouillage du téléphone ou pour la banque en ligne rencontre un taux d'acceptation moins élevé que d'autres usages. C'est une question de se sentir à l'aise, ou de décider collectivement de se sentir mal à l'aise avec certains usages : c'est ce pour quoi les discussions démocratiques sont faites. Nous avons de nombreux choix à faire dans ce domaine, le challenge principal étant d'associer protection et agilité.

Jean Lessi

Secrétaire général de la Commission nationale de l'Informatique et des Libertés

J'ai entendu parler de lisibilité de décisions. La CNIL en 2018 a été la première à réclamer un débat, précisément sur ces nouvelles technologies. Nous avons vu arriver des projets au coup par coup, et nous ne voulions pas découvrir trop tard que notre monde avait changé sans qu'il y ait un choix démocratique global. Et dans ce nécessaire débat, il y a un ordre des questions. Avant que nos ingénieurs ne scrutent ce qui est possible, il faut d'abord s'interroger sur ce qui est souhaitable, la question de l'acceptabilité ne venant qu'à la fin.

C'est le sens de notre contribution de novembre 2019 où nous avons dit quatre choses : quand on ouvre ce débat sain et nécessaire, il faut d'abord resituer la reconnaissance faciale dans une palette d'usages de la vidéo, de la vidéo in-

telligente, des dispositifs de suivi non biométriques des personnes, de la vidéoprotection classique. Il y a parfois confusion, or les enjeux de tous ces domaines diffèrent, pour autant ces technologies peuvent se combiner et les effets peuvent donc s'empiler. Ensuite, dans ce débat, il va falloir mesurer précisément les risques, pour voir ce que le décideur politique veut assumer avec des garanties et ce qu'il ne veut pas assumer. Ces risques ont été rappelés : compromission des données biométriques, les risques liés au degré de surveillance exercé sur les personnes, les risques liés au caractère sans contact de cette technologie et donc sans conscience de son usage, l'ubiquité de nos photos qui peuvent après traitement devenir des données biométriques, etc.

Puis, nous avons rappelé qu'il y a un cadre juridique, qui a des racines certes anciennes mais qui est récent, européen : le RGPD et la Directive Police-Justice. Ce cadre contient déjà des éléments de réponse à une partie de ce débat. Les textes disent schématiquement qu'il faut soit un consentement libre et éclairé, soit un texte pour un motif d'intérêt public important. C'est sur la base de ces textes, que la CNIL a pour mission de faire appliquer, que certains projets ont pu être admis comme PARAFE, alors que d'autres cas d'usage n'ont pas été admis, par exemple les portiques à reconnaissance faciale pour l'accès à des établissements d'enseignement secondaire.

Enfin, la CNIL a rappelé son rôle de régulateur : garante des principes, elle n'est pas le décideur politique. Dans sa mission de conseil, elle rend des avis. Elle a un pouvoir de contrôle et de prise de mesures de correction lorsqu'elle est saisie. La loi française nous a donné en 2016 un pouvoir de regard éthique sur les enjeux liés au numérique. Il nous a semblé souhaitable dans notre avis de novembre de rappeler l'importance que ce débat ait lieu, qu'il ait un certain ordre, et que la CNIL y jouera pleinement son rôle, en toute indépendance, et en laissant le choix final au politique.

Mario Oetheimer

Chef adjoint à l'Unité de recherche et de données de l'Agence des droits fondamentaux de l'Union européenne

Je voudrais insister sur le contexte un peu plus large de la note que nous avons remise à l'échelle européenne. Un peu comme la CNIL, nous avons constaté qu'il était temps de prendre l'ensemble des évolutions en compte afin de discuter des expérimentations qui avaient eu lieu, au Royaume-Uni, en France et en Allemagne. En parallèle, on notait des décisions nationales qui tiraient déjà des conclusions ou réagissaient à certaines initiatives.

En s'appuyant sur la charte des droits fondamentaux, nous avons choisi de prendre un grand angle pour voir, en plus de la vie privée et de la protection des données, quels autres droits pouvaient être impactés par la mise en œuvre des technologies de reconnaissance faciale. Les droits de l'enfant,

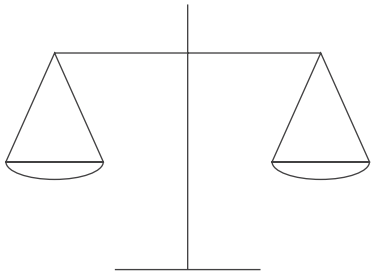
les questions de discriminations sont par exemple à prendre en compte évidemment, mais aussi la question des recours : y en a-t-il un ? Comment l'exercer ?

L'objet de notre rapport était de faire une différenciation entre le présent et l'avenir : l'usage existe, il est encadré, mais avant de franchir un nouveau pas, certains débats doivent avoir lieu.

Les trois initiatives dans les trois pays observés étaient liées au maintien de l'ordre. À part le Royaume-Uni, en avance sur certains domaines, il y a encore de nombreuses questions irrésolues liées à la constitution opaque des bases de données de contrôle. Cela pose des problèmes de droits fondamentaux : comment ces bases ont-elles été élaborées ? sur quels critères ? comment évoluent-elles ?

Les conclusions en Allemagne étaient liées à la question de la régulation. Les forces de l'ordre ont compris que l'intervention du législateur permettrait une discussion et donc augmenterait l'acceptabilité (c'est cohérent avec l'enquête de Renaissance Numérique et de l'Ifop). John Frank a parlé d'une *checklist* nécessaire, c'est notre contribution au débat. Toute autorité publique devrait consulter avant de déployer cette technologie.

L'autre dimension de notre rapport, c'est celle du dialogue entre États membres au niveau européen. Pour l'instant, nous avons surtout constaté un déficit en la matière.



Arthur Messaud

Juriste à La Quadrature du Net

Nous avons entendu des fanatiques de l'État policier, des solutionnistes technologiques, il est bon d'entendre des positions extrémistes. Il suffit d'appliquer le droit comme la CNIL devrait le faire pour voir que tout ce qui a été exposé aujourd'hui n'arrivera pas et relève du rêve, ou d'un productivisme douteux pour gagner quelques secondes dans une file d'attente.

Nous avons publié aujourd'hui une lettre ouverte appelant le Gouvernement et le Parlement à interdire toute utilisation de la reconnaissance faciale à des fins sécuritaires. Nous sommes quatre-vingts organisations à avoir signé ce document et appelons celles et ceux qui le souhaitent à signer également.

Le droit en vigueur en France depuis 2016, c'est la Directive Police-Justice, souvent citée mais pas exposée. L'article 10 parle des données personnelles utilisées dans la lutte contre les infractions et toute autre menace à la sécurité publique : *« Le traitement des données biométriques aux fins d'identifier une personne physique de manière unique est autorisé uniquement en cas de nécessité absolue »*. C'est donc qu'il ne faut y faire appel que s'il n'y a pas d'alternative. Or, dans tous les cas présentés - faire gagner du temps à la police, simplifier les filatures, faciliter les passages aux frontières -, à chaque

fois, c'est faciliter ce qui se fait déjà, donc ce n'est pas une nécessité absolue puisqu'il y a à chaque fois une alternative, qui est un travail humain déjà réalisé aujourd'hui. Les propositions actuelles sont donc contraires à l'article 10. Ce n'est pas une question de proportionnalité, c'est une question de nécessité absolue.

Ce principe n'est pas né par hasard, la nécessité absolue requise pour la reconnaissance faciale sécuritaire a des fondements très classiques face aux abus de la police et des services de renseignement à l'encontre de tout type de militant (gilets jaunes, militants de la cause animale) ou de minorités ethniques. Les limitations matérielles des pouvoirs de la police (filature, suivi de groupes, etc.) sont une garantie contre les abus. On sait que le Gouvernement aimerait aller plus loin dans de nombreux domaines, à l'encontre d'opposants ou de certaines populations. Il ne peut pas le faire parce que les policiers ne sont pas des surhommes. La reconnaissance faciale peut simplifier le travail humain grâce à l'automatisation, réalisant des gains de temps et d'échelle considérables. La limitation technique s'en trouverait balayée. C'est pourquoi les députés européens, dans leur grande sagesse, ont exigé une nécessité absolue pour déployer la reconnaissance faciale. Il n'y a pas de cas où cela s'appliquerait.

Pour les usages privés ou d'agrément, le RGPD s'appliquera simplement : le consentement ou l'intérêt public important. Dans le premier cas et par exemple avec ce que teste Paris Aéroport, ce n'est pas crédible. L'usager devrait pouvoir consentir ou non sans conséquence négative pour lui. Donc le choix sans reconnaissance faciale devrait être aussi agréable et court que le choix avec reconnaissance faciale. C'est contradictoire et antinomique, sauf à mettre des moyens pour mettre les deux choix au même niveau.

Sur la partie intérêt public important, on flirte avec la Directive Police-Justice. PARAFE qui sert au contrôle aux frontières relève de la sécurité publique, même si c'est réalisé par une personne privée. De même pour les écoles : RGPD ou Directive Police-Justice ? Accélérer la file à la cantine ou mettre des caméras à l'entrée ? À chaque fois, ce n'est pas une nécessité absolue : embauchez du personnel et l'objectif sera atteint.

La régulation est sur la table. Notre message à la CNIL est simple : toutes les propositions concrètes aujourd'hui sur la table ne correspondent ni au consentement libre, ni à la nécessité absolue. Dites une fois pour toutes que la reconnaissance faciale n'est pas applicable.

Albane Gaillot

Députée du Val-de-Marne

À l'arrivée de la conclusion des échanges, on voit bien qu'il y a des enjeux très partagés sur la reconnaissance faciale : éthiques, sociétaux. Ces questions, je me les pose comme législateur en prenant de la hauteur. Quel est le projet de société que l'on souhaite ? Quelles garanties pour les libertés ? Faut-il réguler encore plus ?

Aujourd'hui, les citoyens sont très méfiants, les débats sont très clivants et clivés, ce que je dis avec les signataires de mon manifeste pour un moratoire c'est « STOP ». Regardons ce qui existe, les usages. La question n'est pas seulement « comment faire », mais « pourquoi » comme le disait Maître Drouard.

Quel est l'objectif ? Est-ce proportionnel ? Les caméras à l'entrée des lycées sont-elles un véritable enjeu de survie ? Pourquoi ne pas prendre davantage de surveillants plutôt qu'une solution technologique ?

J'ai envie que l'on se pose collectivement la question. L'acceptabilité sociale est cruciale, ce n'est peut-être plus un problème de pédagogie - sortons de la posture professorale - mais d'association concrète des citoyens. On organise de grands débats citoyens sur le climat, pourquoi ne le fait-on pas sur la reconnaissance faciale et d'autres enjeux numériques ? Un moratoire doit permettre ce débat citoyen. L'expérimentation dans les sphères publiques et privées nécessite des cadres, une démarche sincère, une légitimité à le faire, une proportionnalité... et des limites à fixer.

John Frank

Vice-président des Affaires publiques Europe de Microsoft

Je dois réaffirmer qu'il existe d'importants garde-fous, en particulier en ce qui concerne la surveillance de masse. Avant que la police ne commence à utiliser la reconnaissance faciale pour suivre un individu partout où il va, il doit y avoir une prise de décision par un juge, il doit y avoir des vérifications dans le système.

En mars 2018, à Salisbury, Sergueï et Ioulia Skripal ont été attaqués avec un agent neurotoxique. C'était un crime très difficile à comprendre. La police a utilisé la vidéosurveillance pour essayer de repérer les criminels. Elle ne pouvait pas le faire sans l'intervention de la machine : il fallait passer en revue 12 000 heures de bande vidéo. Avec des capacités augmentées, elle a pu identifier deux agents russes. Cela a été fait avec un cadre légal. Mais sans les technologies, elle n'aurait pas pu le faire du tout.

Marine Pouyat

Administratrice de Renaissance Numérique et Consultante, experte en protection des données et vie privée

Comment passer la frontière de l'usage ? Comment adapter la pratique aux besoins ? Plusieurs questions doivent se poser : qu'est-ce que la proportionnalité ? Est-ce que la mesure est appropriée ? Est-ce que la finalité est légitime ? Comment interpréter ce qui est strictement nécessaire ? Comment garantir les libertés individuelles ? La dignité humaine est un principe fondamental inaliénable, au-delà du consentement individuel, comment concilier son respect avec les pratiques de reconnaissance faciale ?

Mario Oetheimer

Chef adjoint à l'Unité de recherche et de données de l'Agence des droits fondamentaux de l'Union européenne

L'analyse de la charte des droits fondamentaux commence par la dignité humaine. La situation de l'individu face à la technologie est clairement déséquilibrée. C'est pourquoi on en a tenu compte pour s'assurer que d'autres garde-fous soient présents. Actuellement, il manque des décisions de justice. On imagine facilement que la Chambre des Lords va se poser des questions par rapport à ce qui se fait au Royaume-Uni. Le balancement pour les autres questions, nombreuses et riches, doit rester ouvert au débat.

Jean Lessi

Secrétaire général de la Commission nationale de l'Informatique et des Libertés

À propos de la décision sur les portiques dans les établissements du secondaire, il y a à la fois nécessité et proportionnalité, et cela nécessite d'ailleurs le consentement. On remplit donc bien toutes les conditions.

Il faut préciser que lorsqu'on protège les données personnelles, il ne s'agit pas seulement de la vie privée. Les données personnelles sont un droit carrefour comme le définit la loi de 1978 et qui inclut la dignité humaine.

Dernier élément pour La Quadrature du Net, c'est très aimable de vouloir nous faciliter le travail. On n'a pas encore vu tous les cas d'usage, par exemple dans le cas de la police judiciaire juste après qu'un crime soit commis. Nous nous prononcerons donc toujours au cas par cas, de manière stable et moderne.

Arthur Messaud

Juriste à La Quadrature du Net

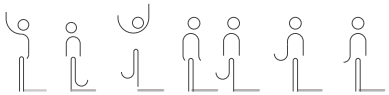
Au-delà de la dignité humaine, on peut s'interroger sur la dignité collective. La reconnaissance faciale privée, par exemple le déverrouillage d'un smartphone, alimente aussi un algorithme qui sert à d'autres usages mal connus. On sait que les premiers bénéficiaires de ces algorithmes enrichis sont les usages sécuritaires.

L'application Mobile Connect, alternative à Alicem proposée par Orange, impose au moment du consentement pour l'usage du visage d'accepter aussi que le visage nourrisse la base algorithmique d'Orange. Est-ce que ces algorithmes équiperont demain des drones policiers ? On n'en sait rien. Même le consentement personnel peut nuire à la collectivité. Cela prouve aussi qu'une entreprise commerciale a tout intérêt à ne pas se fonder sur le consentement libre, pour être rentable le modèle économique doit vicier le consentement pour nourrir un algorithme, qui sera ensuite revendu plus cher pour d'autres usages.

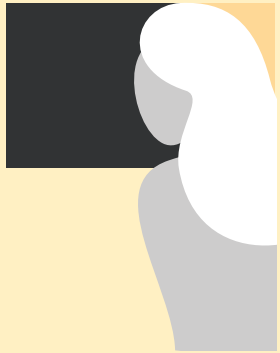
Albane Gaillot

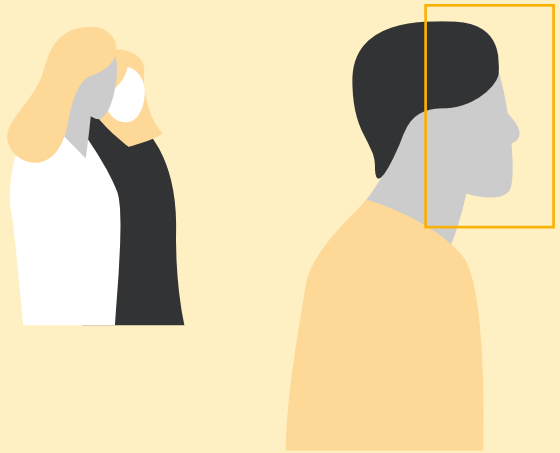
Députée du Val-de-Marne

Qu'est-ce que le consentement ? Cette notion n'est pas que juridique, elle implique une compréhension. Qu'accepte-t-on vraiment ? Est-ce un choix éclairé ? Les opérateurs doivent s'engager vraiment : on sait, par exemple, que les adolescents ne lisent pas les conditions générales d'utilisation trop longues et dans un langage inadapté par rapport à leur envie de se servir de la technologie.



CONCLUSION





Cédric O

Secrétaire d'État chargé du Numérique

Le sujet du jour est très important, il doit donner lieu au maximum de débat public. Je pense d'ailleurs que nous n'en sommes qu'au début de la réflexion. C'est pour moi l'occasion de dire comment au Gouvernement, et moi-même en tant que Secrétaire d'État, nous envisageons les prochaines étapes en matière de reconnaissance faciale.

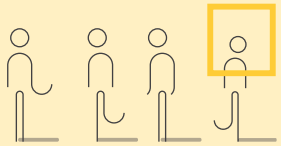
La troisième table-ronde s'est conclue de manière intéressante car elle confirme la règle en matière de numérique : on est toujours dépassé par les usages. D'une part, le consentement ne règle pas la question, en particulier pour les cas où on n'y fait pas appel. D'autre part, parce que le consentement ne protège qu'imparfaitement de certaines utilisations. D'ailleurs, il faut avoir en tête qu'il est déjà possible de modifier la loi au niveau national. Un Gouvernement pourrait ainsi ouvrir la reconnaissance faciale dans des cas bien spécifiques, définis par une loi, pour des raisons de sécurité publique, comme le droit européen le permet. La proportionnalité au regard de la Constitution et du droit européen se poserait, mais c'est théoriquement envisageable. Dans un cadre d'augmentation du risque terroriste et d'une demande croissante de protection de la part de la société, dans le cadre d'un arbitrage de la société entre liberté individuelle et protection d'un genre nouveau, il est donc nécessaire, dans un débat relativement apaisé, de faire des choix collectifs assumés, pour ne pas devoir agir dans l'urgence. Ces débats doivent permettre de dessiner ensemble le choix de la nation, voire au-delà, de l'Europe. .

Il semble nécessaire d'aborder la question de l'efficacité technologique de l'identification. En prenant l'ensemble du spectre des positions, des industriels jusqu'aux associations de défense des libertés numériques, le consensus n'est pas absolu, tant sur le nombre de faux positifs, de reconnaissance des minorités ethniques ou des femmes. Notre approche est donc d'avoir un débat public de manière rationnelle après une phase d'expérimentation, sans tout permettre comme l'a rappelé la CNIL. À titre personnel, je suis partisan des expérimentations sur des périodes de six mois à un an, sous le regard et le contrôle de la société civile, des acteurs technologiques et des chercheurs. Il faudrait que cela soit fait dans un périmètre d'expérimentation public, ce qui permettrait de faire monter en maturité le débat qui reste encore très épidermique -depuis la crainte d'être dépassés jusqu'à crainte d'imiter la Chine -, car sinon la situation ne sera pas sereine : les expérimentations se feront en dehors de ce cadre.

L'usage commercial, avec un consentement même imparfait et incomplet, risquerait de prendre place en dehors de tout débat de société, parce que nous serions dépassés par l'usage. Facebook, Google et Amazon n'ont peut-être pas un usage raisonnable des données, mais en fin de course les gens font appel à ces services. Il faut prendre des décisions après une phase d'expérimentation, avec la participation de toutes les parties prenantes. Les résultats doivent être publics. Tout comme nous avons mené un débat sur la bioéthique avec le Comité consultatif national d'éthique, il doit y avoir un débat de société avec des arbitrages entre des usages, sur des questions de sécurité, de protection des libertés civiles et d'usage. Il faut faire confiance à la démocratie, ne pas céder à des peurs rationnelles ou non, sinon les choses se feront par défaut ou par effraction. La loi peut toujours être changée, évidemment, mais il vaut mieux anticiper.

Il me semble que les questions qui se posent pour l'authentification et pour l'identification sont très différentes. La première pose beaucoup moins de questions d'atteinte à la vie privée et relève rarement d'enjeux de sécurité publique. Elle ne peut se faire qu'avec le consentement. La question de l'authentification est plutôt une question d'encadrement, de capacité de conservation des données, de capacité de vérification des données, d'accès à des services d'authentification, etc. L'identification soulève bien plus de débats. Elle peut se faire sans consentement et les avancées législatives peuvent produire des effets de cliquet : une fois que c'est mis en place, il peut être difficile de revenir en arrière. Et puis l'équilibre entre protection et vie privée est fondamentalement complexe. À ce stade, je n'ai pas d'avis arrêté.

Beaucoup de pays n'ont pas de débat. Et dans ces cas, les majorités changent, les gens changent, les enjeux sécuritaires changent et finalement des décisions sont prises. Je pense qu'il vaut mieux qu'on ait le débat, et qu'il soit rationnel. Croyons-nous ou non dans nos institutions ? Certains intrants considèrent que les institutions dériveront naturellement et qu'on ne peut pas leur faire confiance. Mon sentiment, c'est que l'État et les institutions c'est nous tous. La question qui se pose doit mêler l'usage, les règles. Jusqu'où veut-on aller ? Comment adapter les institutions dans un équilibre entre l'exécutif, le législatif, le judiciaire voire la société civile ? Si nous pensons qu'on ne peut pas faire confiance aux institutions, le débat sera compliqué. Mon sentiment, c'est que nous sommes la société, et que nous devons avoir des institutions à la hauteur des enjeux. Le colloque d'aujourd'hui, particulièrement animé, n'est sûrement que le premier de nombreux autres.



POUR ALLER PLUS LOIN

« Reconnaissance faciale : ce que nous en disent les Français », Renaissance Numérique (décembre 2019).

« La reconnaissance faciale », Note scientifique de l'Office parlementaire d'évaluation des choix scientifiques et technologiques (n°14 - juillet 2019).


Reconnaissance faciale :
Ce que nous en disent les Français

Alors que les technologies de reconnaissance faciale font l'objet d'une médiatisation accrue et s'invitent au coeur du débat politique sur le numérique, le think tank Renaissance Numérique en appelle à ne pas précipiter la réflexion et à prendre le temps de la concertation, sur des technologies dont la mise en oeuvre ne sera pas neutre pour le futur de notre société. Attentif à la préservation de nos libertés publiques dans une société qui se numérise de plus en plus, le think tank a décidé de s'engager dans cette réflexion, au travers de plusieurs travaux. Dans ce document, Renaissance Numérique présente les résultats de l'enquête qu'il a conduite sur la perception des Français vis-à-vis des technologies de reconnaissance faciale, en partenariat avec l'institut Ifop.

Le temps opportun d'un débat public - résultats de l'enquête

Le jeudi 19 décembre, Renaissance Numérique, en partenariat avec le député Jean-Michel Mis, réunissait à l'Assemblée nationale, acteurs publics, privés, de la société civile et du monde de la recherche, pour réfléchir de manière approfondie aux enjeux de la reconnaissance faciale. Dans ce cadre, il semblait nécessaire de ne pas omettre la voix d'un acteur clé, que sont les citoyens. Pour nourrir ces débats, Renais-

RENAISSANCE
numerique

À PROPOS DE RENAISSANCE NUMÉRIQUE

Renaissance Numérique est le principal think tank français indépendant dédié aux enjeux de transformation numérique de la société. Réunissant des universitaires, des associations, des grandes entreprises, des start-ups et des écoles, il vise à élaborer des propositions opérationnelles pour accompagner les acteurs publics, les citoyens et les acteurs économiques dans la construction d'une société numérique inclusive.

Renaissance Numérique
22 bis rue des Taillandiers - 75011 Paris
www.renaissancenumerique.org

Février 2020