LES DISPOSITIFS DE RECONNAISSANCE FACIALE, UN DEFI POUR L'ETHIQUE DE L'INTELLIGENCE ARTIFICIELLE

Thierry Ménissier
(IPhiG, Université Grenoble Alpes)

Résumé

Cet article se donne comme objectif premier de déterminer comment appréhender du point de vue éthique les types de problèmes posés par les dispositifs de reconnaissance faciale, c'est-à-dire par une application particulière des technologies de l'intelligence artificielle (IA). L'objectif secondaire est, à partir de ce cas, de qualifier l'éthique de l'IA à la fois en fonction des contextes sociaux, économique et politique dans lesquels la demande en est exprimée, et en regard de la pluralité des genres d'éthiques. Pour réaliser ce double objectif, l'article caractérise d'abord les dispositifs de reconnaissance faciale ; il produit ensuite une évaluation de leur impact possible sur les libertés privées et publiques à la lumière de la distinction entre « identité » et « personnalité » numériques, et compte tenu du risque de fragilisation qui pèse sur cette distinction cruciale. Enfin, l'article envisage les moyens de garder le contrôle sur de tels dispositifs technologiques en formulant des hypothèses à propos des « lignes de défense » pour contenir les dérives probables ou les mésusages possibles.
Mots-clés : Reconnaissance faciale, intelligence artificielle (IA), biométrie, éthique, liberté.

Abstract

The primary objective of this paper is to determine how to address from an ethical perspective the types of problems posed by facial recognition devices, i.e. by a particular application of artificial intelligence (AI) technologies. The secondary objective is, based on this case, to qualify the ethics of AI both in terms of the social, economic and political contexts in which the demand for it is expressed, and in terms of the plurality of types of ethics. In order to achieve this double objective, the article first characterizes facial recognition devices; it then produces an assessment of their possible impact on private and public freedoms in the light of the distinction between digital "identity" and "personality", and in view of the risk of weakening this crucial distinction. Finally, the article considers ways to maintain control over such technological devices by formulating hypotheses about "lines of defence" to contain likely abuses or possible misuses.
Keywords : Facial recognition, artificial intelligence (AI), biometrics, ethics, freedom.

* * *

Il est aujourd'hui permis de dresser le constat que les dispositifs de reconnaissance faciale se développent rapidement dans les sociétés technologiquement avancées, et également de risquer l'hypothèse que rien ne semble devoir freiner ce développement, tant les organisations (privées et publiques) y trouvent de l'intérêt en termes de commodités (notamment d'efficacité et de sécurité). Parce qu'elles disposent désormais de technologies permettant d'effectuer l'identification et l'authentification des individus de manière à la fois efficace, permanente et invisible, elles peuvent offrir à leurs clients (pour les entreprises) ou à leurs administrés (pour les Etats et les collectivités) des services qui permettent à ceux-ci de vivre dans la quiétude. Du moins, c'est en cela que semblent consister à la fois la promesse et la tentation offertes par ces technologies.

Or, l'une comme l'autre apparaissent séduisantes mais également inquiétantes, compte tenu de la nature des technologies engagées ainsi que de leur mise en relation avec des bases de données déjà constituées ou susceptibles de l'être, et compte tenu, aussi, de la sous-qualification éthique et politique dont ces bases de données sont aujourd'hui l'objet. En dépit de l'émotion que suscite dans le débat public le déploiement des dispositifs de reconnaissance faciale (émotion relayée par une importante activité médiatique), les évaluations éthiques approfondies de ces technologies sont rares.

Cette contribution se propose d'abord de déterminer comment appréhender du point de vue éthique les types de problèmes posés par de tels dispositifs. Tel est le premier objectif de cet article. Or, comme ces dispositifs représentent une application particulière des technologies de l'intelligence artificielle (IA), l'objectif secondaire de cet article est, en partant de ce cas d'espèce, de contribuer à la qualification de l'éthique de l'IA en fonction des contextes sociaux, économique et politique dans lesquels la demande en est exprimée, et également en regard de la pluralité des familles de l'éthique. Cette démarche est justifiée par le fait que l'absence d'évaluation approfondie des dispositifs de reconnaissance faciale et de biométrie (et plus généralement des technologies de l'IA) profite aujourd'hui à un seul type d'analyse éthique, celui proposé par la tradition utilitariste. Une telle situation tend à laisser dans l'ombre un certain nombre de problèmes sensibles à l'opinion publique, mais non appréhendés par l'éthique alors qu'il serait nécessaire de les soumettre à un tel traitement. Le traitement des cas par le seul utilitarisme, c'est-à-dire le fait que l'IA demeure impensée autrement que sous cet angle particulier, produit certains effets que nous allons souligner.

Pour réaliser le double objectif que se donne l'article, nous allons dans un premier temps caractériser les dispositifs de reconnaissance faciale ; puis, dans un second, proposer une évaluation de

leur impact possible sur les libertés privées et publiques à la lumière de la distinction entre « identité » et « personnalité » numériques, et compte tenu du risque de fragilisation qui pèse sur cette distinction cruciale. Enfin, on envisagera les moyens de garder le contrôle sur de tels dispositifs technologiques en formulant des hypothèses à propos des « lignes de défense » pour contenir les dérives probables ou les mésusages possibles[1].

Les dispositifs de reconnaissance faciale, des technologies biométriques, aisément connectables aux flux de méga-données

Les dispositifs de reconnaissance faciale relèvent des technologies biométriques. On entend par ce terme des systèmes techniques associant automatiquement des données captées à partir du corps ou de la présence des individus et la caractérisation de ces derniers par le biais des informations collectées[2]. Dans le cas de la reconnaissance faciale, la captation automatique de la forme des visages (par captation directe ou à partir d'un artefact, par exemple une photo ou une vidéo) permet d'authentifier ou d'identifier la personne à qui appartient ce visage, tandis que d'autres types de système réalisent la même opération à partir du contact des empreintes digitales, de la lecture des iris, de la saisie de la voix humaine, etc. Schématiquement, ces dispositifs fonctionnent en deux temps : premièrement, une collecte initiale de données est nécessaire pour permettre l'établissement d'un « gabarit », à savoir, un modèle informatique représentant certaines caractéristiques de ce visage : deuxièmement, ce « gabarit » est utilisé pour authentifier ou identifier la personne dans les situations concrètes. Parmi les dispositifs biométriques, la reconnaissance faciale occupe une place à part, car elle permet de capter des données issues du corps humain sans contact ni consentement préalable, tandis que pour d'autres systèmes, il faut prononcer des paroles de manière claire et distincte (reconnaissance vocale), approcher son œil d'un viseur (reconnaissance oculaire), imprimer les empreintes de ses doigts (reconnaissance digitale), ou bien donner un échantillon de salive ou de sang (prélèvement d'ADN).

Les dispositifs qui permettent l'authentification des personnes à partir de la captation des images des visages sont d'ores et déjà largement utilisés dans des opérations de la vie ordinaire tel que le filtrage des accès et la sécurité, par exemple dans ces cas :

---

[1] Cet article est le fruit du travail scientifique qui est mené dans le cadre de la chaire « éthique & IA » soutenue par l'institut pluridisciplinaire en intelligence artificielle MIAI@Grenoble Alpes (ANR-19-P3IA-0003).

[2] Voir Meryem Marzouki, « Biométrie : corps étrangers sous contrôle », *Plein droit* n° 76, mars 2008, p. 24-26 : « La nouveauté de la biométrie réside dans l'automatisation de la mesure et de la reconnaissance des caractéristiques d'un individu, c'est-à-dire dans le couplage entre anthropométrie et informatique. » (p. 26).

-Ouverture de sessions personnelles sur les terminaux électroniques (PC, tablettes, smartphones) et autorisation d'accès à des espaces, tels des lieux physiques ou à des sites numériques estimés sensibles : manifestations ou lieux publics, administrations et institutions (prison, enseignement, religions, etc.), banques, santé, sécurité sociale et assurances, etc.

-Autorisation d'accès à des lieux ou à des sites qui impliquent que le requérant soit accrédité et « en règle » : entreprises devant protéger leur activité contre le vol de leurs actifs, toutes les applications payantes…

Ils sont également employés pour l'identification générique des personnes ; par exemple lorsqu'il s'agit de surveiller une foule comme dans le cas de très nombreux aéroports internationaux ou lors du récent Carnaval de Nice, ils permettent de retrouver des personnes estimées dangereuses en les distinguant automatiquement des autres à partir de leur gabarit.

Dans tous les cas, on pourrait dire, en s'inscrivant dans la perspective d'un travail de distinction conceptuelle classique, qu'il y a ici une *identification* des individus, mais que ce n'est pas une identification des personnes, ou « *personnification* ». En procédant de la sorte, on retrouve le type de travail philosophique que fit John Locke au XVIIème siècle dans l'*Essai sur l'entendement humain*[3], qui a permis de construire une différence ontologique entre l'identité de l'individu (qualifiable extérieurement par son nom ou ses attributs apparents) et celle de la personne (caractérisée par ses états internes, corporels et mentaux).

Un individu humain, c'est un nom et un état civil ; une personne, c'est un ensemble de vécus, d'opinions, d'expressions diverses, variées et potentiellement contradictoires entre eux. L'individu concerne l'assignation à des éléments extérieurs et contingents, la personne renvoie à l'authenticité d'un vécu multiple. « Identifier » et « personnifier » un individu constituent normalement deux actions différentes, la première assigne l'individu à des déterminants contingents ou extérieurs à ce qu'il est au fond de lui (tels que son nom, son âge et son lieu de naissance, son sexe biologique – toutes choses non choisies et parfois subies) ; la seconde représente une caractérisation plus intime (ce qu'il ressent et ce qu'il pense, ses états d'âme et ses convictions profondes, ses choix intimes de culture et de vie, ses options éthiques personnelles).

Or, il nous faut ici avancer d'un pas, et remarquer qu'en dépit des apparences, la reconnaissance faciale, à l'instar des autres systèmes biométriques, non seulement identifient les individus, mais également sont susceptible de les « personnifier », c'est-à-dire d'intégrer pleinement la vie des personnes. Au point où nous en sommes déjà aujourd'hui, en effet, les dispositifs biométriques

[3] John Locke, *Essai sur l'entendement humain* (1689), livre II, chapitre 27, trad. J.-M. Vienne, Paris Editions philosophiques J. Vrin, 2001, p. 505-542.

facilitent l'exercice de l'identification à partir de la captation des données personnelles, et de ce fait, en étant susceptibles d'intégrer des éléments bien plus riches que l'identité stricto sensu, ils sont en mesure d'interférer plus intimement avec la personnalité individuelle. Ces données sont variées et peuvent concerner, outre la validation de l'identité des individus,

-le relevé de la localisation de ces derniers dans l'espace,

-le suivi de la chronologie de leurs activités,

-l'identification de la nature leurs activités.

Si l'on n'y prête un soin extrême, ces données de base, constituables à partir d'une captation désormais techniquement aisée, peuvent se trouver corrélées à d'autres données, confidentielles ou secrètes, détenues par des opérateurs d'IA publics et privés :

-celles liées à l'activité bancaire et à la situation fiscale des personnes,

-celles contenues dans leur casier judiciaire,

-celles contenues dans leur dossier médical,

-celles détenues par les assureurs et les mutuelles,

-celles détenues par les services de sécurité (polices nationales et municipales, services secrets intérieurs et extérieurs),

-celles détenues par les employeurs (publics ou privés) des personnes,

-celles détenues par les compagnies privées tels que celles qui utilisent les réseaux (opérateurs de téléphonie et de services numériques, réseaux sociaux, commerçants variés) – ces dernières sont susceptibles de révéler les orientations des personnes et de donner accès à leurs opinions ordinairement tues ou tenues secrètes.

Ces deux séries de données peuvent enfin se trouver associées à celles produites en temps réel par les terminaux utilisés (smartphones, PC, tablettes) mais également, dans le contexte du déploiement de ce qu'on appelle l'« internet des objets » (ou *IoT*), par les objets connectés qui sont en contact avec les personnes et qui « communiquent » à travers leur activité : transports privés (automobile, moto, vélo, etc.) ou publics (trams, trains, avions…), appareils électroménagers (réfrigérateurs, système d'éclairage et de chauffage, dispositifs de remise en forme personnels…), bâtiments connectés, etc. En reprenant la distinction lockéenne, on pourrait dire que ces nouveaux ensembles offrent un cadre inouï pour l'identification des individus, mais également pour leur « personnification », concept qu'il faudrait entendre d'un double point de vue : d'une part, les es-

paces (physiques et numériques) offrent aux individus des accès et des services, de l'autre, ils monitorent leur activité et enregistrent des données qui, agrégées en flux de mégadonnées (*big data*), ont une forte pertinence en termes de renseignement sur l'intimité et par conséquent une certaine importance en termes policiers et marchands. Or, du point de vue du déploiement de l'*IoT*, n'importe quel lieu (privé ou public), n'importe quel dispositif socio-technique (tels un véhicule pour l'action de se déplacer, un fauteuil ou un matelas pour celle de se reposer) sont susceptibles de devenir un outil pour l'identification et la personnification.

Au-delà de la captation des données par la reconnaissance faciale et par les autres dispositifs biométriques actuels, s'ajoutent aujourd'hui la collecte d'un type d'informations qui les rendent potentiellement encore plus efficients : celles qui touchent à la captation des données corporelles ou biologiques. Ce type de données concernent, d'une part, les comportements perceptibles par des capteurs plus sensibles et objectifs que ne peuvent être les sens humains normaux (ainsi, la perception et la mesure du pouls qui s'accélère, celles de la sudation accrue, celles de la dilatation des pupilles, etc.) ; et de l'autre, les informations véhiculées par le sang ou l'ADN des personnes, deux substances qu'il est éventuellement possible de recueillir et d'analyser à l'insu des personnes.

Il serait difficile de soutenir que la mise en relation de toutes ces *data* ne représente pas, au-delà de la simple authentification, une possibilité de constituer des bases de données permettant de connaître une personne à travers ses comportements. Les dispositifs de reconnaissance faciale fournissent en tout cas à ces bases de données l'occasion d'être actives pour toute sorte de situations, déjà bien réelles en France[4] comme à l'étranger, telles que la reconnaissance des personnes participant à une manifestation politique[5].

Les dispositifs de reconnaissance faciale augmentent considérablement le risque de mise en œuvre d'une société de surveillance intégrale et invisible

Dans ces conditions, l'inquiétude grandit légitimement pour la préservation tant de l'intégrité de la sphère privée que de la capacité de circulation des personnes : l'intimité, le secret personnel, les

[4] Voir à propos du fichier TES (ou « titres électroniques sécurisés », qui sert à l'établissement des papiers d'identité français), François Pellegrini et André Vitalis, « La création du fichier biométrique TES : la convergence de logiques au service du contrôle », Sociologie, n°4, vol. 8/2017, consulté le 16/12/2019 (https://journals.openedition.org/sociologie/3394).

[5] Ainsi, le site de lanceurs d'alerte La Quadrature du Net révélait-il récemment que le gouvernement français a progressivement mis en œuvre un système capable d'identifier et de fournir des données sur les manifestants, qui met en relation la reconnaissance faciale et les bases de données des fichiers TAJ (« traitement des antécédents judiciaires » qui comprend les éléments contenus dans les casiers judiciaires individuels) et TES, et ceux collectés dans le cadre de la loi du 24 juillet 2015 relative au renseignement. Voir La Quadrature du Net, 18/11/2019, « La reconnaissance faciale des manifestant.e.s est déjà autorisée » (https://www.laquadrature.net/2019/11/18/la-reconnaissance-faciale-des-manifestants-est-deja-autorisee/), consulté le 4/12/2019.

libres allées et venues courent évidemment de grands risques, d'autant plus que ces technologies se trouvent sinon déjà connectées, du moins connectables d'une part à des réseaux denses de caméras de surveillance urbaine, et de l'autre aux flux de *data* engendrées à propos des personnes ou par les personnes elles-mêmes. Avec la reconnaissance faciale généralisée, on pourrait dire que l'espace social tend à devenir transparent ; de manière tendancielle, ils transforment les espaces qui leur sont offerts en espaces de visibilité intégrale. Ici, il apparaît très difficile ne pas analyser la mise en œuvre de ces dispositifs à l'aune de la problématique du pouvoir. Mais comment entendre plus précisément ce dernier terme ?

La reconnaissance faciale, telle qu'elle est actuellement déployée, concerne plus précisément trois formes connues du pouvoir, qui se trouvent ainsi actualisées. Premièrement, il y a un risque de surveillance généralisée des individus, comme le ferait un grand panoptique, selon le dispositif autrefois inventé par Jeremy Bentham, puis analysé par Michel Foucault dans son livre sur la naissance de la prison et dont il fait un symbole du pouvoir à l'époque contemporaine[6]. Par extension et pour reprendre les termes foucaldiens en référence à l'analyse du panoptique, les dispositifs de reconnaissance faciale pourraient être rattachés à la volonté de « discipliner » les agents sociaux, en les assignant, *via* l'identification et la « personnification » auxquelles ils contribuent, à des normes s'exerçant sur leurs comportements. Mais cette manière de concevoir l'expression du pouvoir, si elle constitue comme la toile de fond d'une surveillance généralisée possible, régulatrice des conduites individuelles, n'est pas la seule ni sans doute la plus pertinente pour comprendre le déploiement des dispositifs de reconnaissance faciale. Car, deuxièmement, ce déploiement peut également être caractérisé comme l'expression de la volonté d'agir sur les conduites des populations *via* une action sur les milieux dans lesquels elles évoluent : il est de la sorte susceptible d'être analysé à l'aune des notions foucaldiennes de biopouvoir et de biopolitique[7]. Troisièmement, on peut également les soupçonner, en reprenant les travaux de Jean-Gabriel Ganascia à propos de la manière dont, dans un réseau numérique, chacun contribue à apporter spontanément, volontairement ou involontairement, des données d'information, de nourrir le système « catoptique » ce qui engendre de la « sousveillance » à la fois auto-contributive, généralisée, permanente, et invisible[8].

---

[6] Michel Foucault, *Surveiller et punir. Naissance de la prison*, Paris, Gallimard, 1975.

[7] Michel Foucault, *Sécurité, Population, Territoire, Cours au Collège de France, 1977-1978*, Édition établie sous la direction de François Ewald, Alessandro Fontana et Michel Senellart, Paris, Gallimard-Le Seuil, 2004 ; *Naissance de la biopolitique, Cours au Collègue de France*, 1978-1979, Édition établie sous la direction de François Ewald, Alessandro Fontana et Michel Senellart, Paris, Gallimard-Le Seuil, 2004.

[8] Jean-Gabriel Ganascia, *Voir et pouvoir : qui nous surveille ?*, Paris, Editions Le Pommier, 2009.

Ces outils issus de la théorie du pouvoir apparaissent d'autant plus importants pour l'analyse des dispositifs de reconnaissance faciale qu'on voit en ce moment apparaître des systèmes entiers dans lesquels les effets de la reconnaissance faciale (ainsi que tous les autres dispositifs biométriques) prennent une tout autre dimension. Ces systèmes, ce sont les « *smart cities* », ensembles urbains et sociaux intégralement outillés dès leur conception dans le but explicitement formulé de capter les données afin de mieux distribuer et d'optimiser les flux (d'énergie, d'eau, de l'air des climatiseurs, de transport, financiers et touchant alimentation)[9]. Si ces ensembles urbains, dans les projets des entreprises en bâtiment et selon les planificateurs urbanistes contemporains, ont été conçus comme des *ensembles sociaux*, ils n'ont encore jamais été conçus comme des *ensembles politiques*, c'est-à-dire qu'ils favorisent une idée d'autonomie plutôt liée au rapport à l'environnement que tournée vers la demande humaine d'autonomie, laquelle se décline notamment en termes d'imputation de responsabilité civique, d'aspiration à l'équité, et de participation politique en vue de l'autodétermination. Conçue pour être efficace du point de vue sécuritaire et environnemental, la ville intelligente n'est pas encore « intelligible »[10], c'est-à-dire réflexive, critique et démocratique. Une *smart city* « intelligible » serait politique, car elle favoriserait le fait que les dispositifs techniques déployés permettent à chacun, via des « données ouvertes » (*open data*) rendues utiles aux citoyens par des programmes pédagogiques dédiés, de comprendre leur action en associant plusieurs niveaux (par exemple, en s'efforçant de relier les données collectées à des valeurs et à des finalités clairement formulées) et d'exprimer leur choix de vie réfléchis, à parité avec les autres.

Les dispositifs de reconnaissance faciale renvoient donc aux trois niveaux de l'analyse du pouvoir. D'abord le pouvoir comme contrôle tendant à discipliner les individus ; grâce à eux, tout individu peut être singularisé, et de ce fait, aisément considéré comme suspect à un titre ou à un autre. Les méga-données sont en effet susceptibles de révéler tous les excès (petits et grands) des individus en termes de conduite, et d'attirer l'attention sur les petites ou grandes déviances par rapport à la norme statistique ou aux contraintes exprimées par les autorités en place dans les organisations publiques et privées. Par suite, au sein des *smart cities* où les espaces physiques et numériques se rejoignent sans cesse et composent un seul et même espace, tout individu pourra donc être à la fois identifié et « personnifié » non seulement par les services de sécurité et de police,

[9] Pour une analyse socio-politique des *smart cities*, voir Antoine Picon, *Smart Cities : Théorie et critique d'un idéal auto-réalisateur*, Paris Editions B2, 2013 ; Jean-Bernard Auby, Vincenzo De Gregorio (dir.), *Données urbaines et* Smart Cities, Paris, Editions Berger-Levrault, 2017.

[10] Emmanuelle Caccamo, Julien Walzberg, Tyler Reigeluth et Nicolas Merveille (dir.), *De la ville intelligente à la ville intelligible*, Québec, Presses de l'Université du Québec, « Cahiers du GERSE », 2019.

mais également par tous les services afférents aux conditions de son existence, concernant la rectitude de son action au sein de son « milieu de vie » (physique et numérique). Il convient ici de mobiliser la deuxième définition du pouvoir en intégrant à la première le caractère collectif du rapport aux milieux via la distribution des flux. Parce qu'ils agissent sur la relation des populations à leurs milieux, ces dispositifs sont pleinement ouverts à la gestion des populations par le biopouvoir. Du fait de l'intrication des milieux physiques et numériques ainsi que de l'auto-contribution des usagers du numérique, ils le sont également à leur identification/personnification en termes de sous-veillance, et renvoient donc à la troisième définition du pouvoir.

Dans les *smart cities*, le contrôle peut s'effectuer automatiquement : le système autorise les accès aux individus sans problèmes et les verrouille pour ceux qui sont suspects. Dans ces conditions, la meilleure image possible, pour une analogie avec l'architecture, pourrait être celle d'un gigantesque labyrinthe multidimensionnel. C'est en un tel labyrinthe que se transforme l'espace physique aussi bien que numérique régi par le système global dans lequel les dispositifs automatiques peuvent *distinguer* donc *discriminer* n'importe quel individu pour de « bonnes » ou de « mauvaises » raisons qui, parce qu'elles sont effectuées « en temps réel » ne seront pas examinées ni discutées au moment où il conviendra de le faire, c'est-à-dire au moment du blocage de l'accès. En tant que tel, ainsi que l'a dénoncé Woodrow Hartzog, Professeur à la Faculté de droit de la Northeastern University à Boston, les dispositifs de reconnaissance faciale représentent « le parfait outil pour l'oppression »[11], validant ainsi les analyses inquiètes exprimées sur le plan de la sociologie et dans le champ des « *Surveillance Studies* » par David Lyon[12].

L'illusion de remplacer le politique par le technologique

Le développement actuel de la reconnaissance faciale interpelle par conséquent la philosophie politique, du fait qu'il menace la vie privée en faisant courir le risque d'un viol de l'anonymat auquel chacun a droit dans une démocratie et qui permet d'élaborer une pensée réellement personnelle et originale. Au vu de quoi, les agences chargées de la préservation des droits fondamentaux des personnes, qu'elles soient publiques ou non-gouvernementales, ont récemment réagi : ainsi, l'Agence Européenne pour les Droits fondamentaux a rendu un avis qui s'alarme de l'usage de

[11] Woodrow Hartzog, « Facial Recognition Is the Perfect Tool for Oppression », *Medium*, 2/08/2018, accessible à l'URL : https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66, consulté le 15/12/2019.

[12] Cf. David Lyon, *The Electronic Eye: The Rise of Surveillance Society* - Computers and Social Control in Context, Minneapolis, University of Minnesota Press, 1994 ; David Lyon & Colin Bennet (eds.), *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*, Londres, Routledge, 2008 ; David Lyon, *Identifying Citizens: ID Cards as Surveillance*, Cambridge, Polity Press, 2009.

technologies pouvant échapper à tout contrôle et comprenant de nombreux biais[13]. Une organisation fameuse pour la défense des libertés démocratiques, l'ACLU (American Civil Liberties Union), a solennellement demandé à la police de Détroit, Michigan, de ne pas déployer de tels dispositifs[14] au motif que ces derniers font peser sur les populations des risques accrus de discrimination en fonction de la couleur de peau et, globalement, ils mettent en danger le droit à l'anonymat dont se nourrit la vie privée. En France, la Commission Nationale Informatique et Libertés a appelé à un débat public de fond engageant les valeurs de la démocratie[15]. Enfin, du côté des lanceurs d'alerte, le site La Quadrature du Net a souligné à plusieurs reprises, dans des contributions approfondies, les multiples dangers de l'usage massif de ces dispositifs[16].

Si le déploiement des dispositifs de reconnaissance faciale représente un danger majeur, c'est également du point de vue de l'illusion sur laquelle ils sont construits : on ne saurait en effet sans grand risque remplacer « l'esprit de la cité » (à savoir, l'intention politique, celle qui anime le débat collectif dans le projet démocratique) par des systèmes techniques. En effet, vouloir réaliser un tel programme évoque, dans l'esprit d'une philosophie éthique et politique sensible aux expérience du passé, celui des tentatives totalitaires, lorsque, d'abord dans l'Italie fasciste, puis dans la Russie stalinienne et en Allemagne nazie dans le premier tiers du XXème siècle, des organisations autoritaires ont voulu maîtriser les oppositions qui leur étaient faites au niveau d'Etats-nations, et cela par tous les moyens techniques possibles et grâce à l'autocontrainte engendrée par l'idéologie, donc selon un processus conjuguant le niveau technologique et des dispositifs psycho-sociaux produisant des effet d'assujettissement extrêmement efficaces ainsi que l'a bien montré Hannah Arendt dans le troisième tome des *Origines du totalitarisme*[17]. *Mutatis mutandis*, les dispositifs de reconnaissance faciale d'aujourd'hui font courir le même risque que les techniques d'encadrement déployés dans les Etats totalitaires d'autrefois, mais ils le font au sein de sociétés apparemment

[13] Voir European Union Agency for Fundamental Rights, « Facial recognition technology: fundamental rights considerations in the context of law enforcement », 27/11/2019, accessible à l'URL : https://fra.europa.eu/en/publication/2019/facial-recognition consulté le 15/12/2019.

[14] ACLU Condemns Detroit Board of Police Commissioners' Vote to Approve Detroit Police Department's Facial Recognition Technology Policy », 19/09/2019 : https://www.aclu.org/press-releases/aclu-condemns-detroit-board-police-commissioners-vote-approve-detroit-police, consulté le 11/12/2019.

[15] *Reconnaissance faciale. Pour un débat à la hauteur des enjeux*, 15/11/2019, accessible à l'URL : https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux, consulté le 19/12/19.

[16] Voir par exemple La Quadrature du Net, « Le vrai visage de la reconnaissance faciale », 21/06/2019, accessible à l'URL : https://www.laquadrature.net/2019/06/21/le-vrai-visage-de-la-reconnaissance-faciale/ consulté le 11/12/2019.

[17] Hannah Arendt, *Les Origines du totalitarisme* (1951), tome III, chapitre 13 : « Idéologie et terreur », éd. sous la dir. de P. Bouretz, Paris, Gallimard, 2002.

démocratiques, avec l'alibi des séductions de l'innovation technologique : la performance technologique au service du confort des individus qui effectuent des choix de consommation de manière apparemment libre – mais non réflexive, non critique. Dans les deux cas, le moyen est comparable et l'intention semble la même. Le moyen consiste à dépolitiser la société au profit du confort « bourgeois », et l'intention vise à faire abandonner l'exigence imposée par « l'esprit de la cité », laquelle se traduit par la volonté d'entrer dans le débat démocratique afin de favoriser les disputes fécondes pour la liberté.

Cette mise en garde contre le déploiement de la reconnaissance faciale peut s'étendre à l'usage des technologies biométriques, dont on n'a pas manqué, depuis une dizaine d'années, de souligner les dérives possibles en termes de contrôle et de danger pour les libertés[18]. Elle peut également être entendue à l'aune de la dénonciation de l'illusion techniciste comme l'avaient fait en leur temps Lewis Mumford[19] et Jacques Ellul[20]. En dépit de cela, si le déploiement de la reconnaissance faciale progresse, c'est qu'à l'instar des autres dispositifs biométriques, ils bénéficient de la complicité des usagers qui, par désir de confort ou par les séductions du narcissisme, les admettent dans les espaces publics (aéroports, grands magasins, etc. semblent de la sorte mieux sécurisés) et les adoptent en tant que systèmes d'accès de leurs terminaux (il est plus facile de se laisser identifier par le système technique que de mémoriser et de saisir les codes d'accès à ce système). Cette attitude d'acceptation spontanée apparaît d'autant plus curieuse qu'elle configure un mode étroit de l'identité, qui se superpose – et c'est un autre paradoxe – à des postures contemporaines où le moi « digitalement étendu », se nourrit des fictions que sont ses propres avatars dans la sphère numérique[21]. La biométrie assigne l'identité à une stricte univocité, tandis que dans le monde numérique, elle est susceptible de se diversifier à l'infini.

En renonçant de la sorte à ce qui reste de leur droit à demeurer anonymes, les usagers-consommateurs de biométrie domestique renoncent au bienfait d'une autre attitude, qui, parce qu'elle bénéficie d'une forme assumée et bienfaisante de solitude, n'est suspecte d'être ni conformiste ni

---

[18] Les critiques des systèmes biométriques ont été par exemple développées par les contributions suivantes : Ayse Ceyhan, « Enjeux d'identification et de surveillance à l'heure de la biométrie », *Cultures & Conflits* [En ligne], 64, hiver 2006, accessible à l'URL : http://journals.openedition.org/conflits/2176 consulté le 13/12/2019 ; Ayse Ceyhan, Pierre Piazza (dir.), *L'identification biométrique. Champs, acteurs, enjeux et controverses*, Paris, Editions de la Maison des Sciences de l'Homme, 2011 ; Gérard Dubey, « Nouvelles techniques d'identification, nouveaux pouvoirs. Le cas de la biométrie », *Cahiers internationaux de sociologie*, 2008/2 n° 125, p. 263-279.

[19] Lewis Mumford, *La Transformation de l'Homme* (1956), trad. B. Pêcheur, Paris, Editions de l'Encyclopédie des Nuisances, 2008 ; « Technique autoritaire et technique démocratique » (1963), trad. A. Gouilleux, in *Notes et morceaux choisis. Bulletin critique des sciences, des technologies et de la société industrielle*, n°11, 2014, p. 109-121

[20] Jacques Ellul, *Le Bluff technologique*, Paris, Hachette Littératures, 1988.

[21] Voir à ce propos David M. Barry, « Subjectivités computationnelles », *Multitudes*, 2015/2 n°59, p. 196-205 ; Russel W. Belk, « Extended Self in a Digital World », *Journal of Consumer Research*, Vol. 40, n°3 (Octobre 2013), p. 477-500.

manipulée. Tel est ce parti qu'avait pris Descartes, qui en témoigne dans le passage fameux du *Discours de la méthode* (1637) où il écrit avoir « pu vivre aussi solitaire et retiré que dans les déserts les plus écartés ». Le philosophe exprimait par-là comment, afin d'élaborer une philosophie qui bouleversait tout ce qu'on savait à son époque, il lui avait semblé commode de bénéficier d'un droit à l'anonymat, en évoluant inconnu au milieu de la foule d'Amsterdam, « grand peuple actif, et plus soigneux de ses propres affaires que curieux de celles d'autrui »[22]. Si cette allusion de Descartes à ses conditions de vie dans les Provinces-Unies signifie pour notre situation contemporaine quelque chose d'important, c'est que le fait de jouir d'un espace favorable à la quiétude de l'anonymat, cette condition minimale de la liberté privée, constitue un bien public et représente le fruit de l'activité politique des humains, et ne saurait être envisagé comme l'effet neutre de leur seule ingéniosité technique.

Conclusion

La définition et la constitution d'une éthique de l'IA se trouvent mise au défi par la reconnaissance faciale. Celle-ci semble représenter un cas d'espèce qui apparait immédiatement bien plus ambigu que d'autres, tels que le « véhicule autonome » (terrestre, maritime ou aérien) ou la *smart city* ; du moins révèle-t-il mieux que les autres les dangers que la civilisation humaine encourt à privilégier de manière systématique les dispositifs automatiques à la place des actions humaines.

Le danger que font courir pour les libertés publiques et privées les dispositifs de reconnaissance faciale, pointe avancée des capteurs biométriques, est susceptible de s'accroitre rapidement, sous l'effet de trois types de facteurs. D'abord, il faut souligner l'effet du développement technologique (celui de l'*IoT*, celui des capteurs d'émotions). Ensuite, il convient de relever la corrélation entre ce développement et l'émergence de marchés ouverts aux organisations (privées et publiques) et aux consommateurs particuliers. Enfin, la faiblesse de l'évaluation éthique dominante ramène la démarche éthique à la prise de décisions particulières sous la condition d'une acceptation globale des technologies efficaces mises en circulation sur les marchés. Ces facteurs conjugués induisent deux conséquences possibles : le déploiement massif des dispositifs de reconnaissance faciale et le fait que les capteurs biométriques non seulement permettront l'identification/authentification des individus, mais également délivreront une connaissance de leur personnalité.

[22] René Descartes, *Discours de la méthode* (1637), in *Œuvres philosophiques*, tome I, édition de Ferdinand Alquié, Paris, 1963.

L'évaluation éthique de tels dispositifs constitue donc un « problème méchant » (ainsi qu'on en a récemment proposé l'idée[23]. « *Wicked Problems* » est un concept promu en 1973 par Rittel et Webber qui désigne des problèmes difficiles à définir et caractérisés par une résistance à la résolution, basés sur des jugements de valeur et, au mieux, qui offrent des solutions nécessitant un redéveloppement constant et qui sont par nature politiques, engageant des choix de valeurs explicites[24]. Si la situation apparaît d'une certaine gravité, c'est de plus parce qu'avec le regard, le visage humain représente pour chacun d'entre nous la plus importante interface entre l'intime et le social. Toute une tradition éthique se rattache à devenir ou à rester pleinement humain en acceptant la demande que nous fait autrui par son visage, et en assumant l'altérité irréductible de l'autre par le biais de son visage, différent du mien, face au mien. Ainsi que l'écrivait Lévinas, auteur d'une éthique visant à conjurer les risques de voir, après la Shoah, revenir des conduites inhumaines, *« le visage s'impose à moi sans que je puisse rester sourd à son appel, ni l'oublier, je veux dire sans que je puisse cesser d'être responsable de sa misère. »*[25]*. En s'inspirant de cette thèse, on pourrait estimer que parce que les usagers délèguent le souci de leur sécurité et leur bien-être à des systèmes qui schématisent les visages humains via le travail des algorithmes, se profile aujourd'hui le risque d'oublier l'injonction à rester humain grâce au face à face entre personnes. En termes lévinassiens, le risque engendré par le déploiement de la reconnaissance faciale repose sur le fait que ce dernier favorise le déni techniciste du caractère profondément éthique de la relation interindividuelle, ce caractère que nous rappelle sans cesse, dans sa singularité et son altérité, le visage d'autrui. Si la question de la reconnaissance faciale apparaît d'une certaine gravité, c'est, au-delà de ses aspects pragmatiques du point de vue éthique et politique, en raison du sentiment qu'une limite anthropologique est irrémédiablement franchie, les humains se trouvent désormais exposés à un risque éthique majeur.*

Aussi, face à une telle menace, pourrions-nous émettre deux recommandations. D'abord, se dessine une ligne de défense nécessaire sur le plan de l'usage social des dispositifs de reconnaissance faciale, qui apparaît nécessaire et importante bien que fondamentalement fragile. Il convient que les personnes identifiées car soumises à ces dispositifs le soient en connaissance de cause, voire en expriment le consentement. Il serait aisément possible de demander aux autorités de surveillance/sécurité/police l'obligation de l'information (par exemple en signalant par un pictogramme

[23] « […] ethical considerations in AI are dominated by 'Wicked Problems' », Sarah Joy Bennett, « Investigating the Role of Moral Decision-Making in Emerging Artificial Intelligence Technologies », CSCW'19 (Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing, p. 28-32), November 9-13, 2019, Austin.

[24] Horst W. J. Rittel, Melvin M. Webber, « Dilemmas in a General Theory of Planning », Policy Sciences, Vol. 4, n° 2, 1973, p. 155-169.

[25] Emmanuel Lévinas, *Humanisme de l'autre homme*, Editions Fata Morgana, *1972, p. 49.*

dédié les espaces et lieux publics soumis à la reconnaissance automatique). De son côté, le respect du consentement personnel peut constituer un degré supplémentaire de régulation, qui pourrait concerner certains espaces ou lieux publics tels que les accès des entreprises ou les guichets des administrations. Par ailleurs, seul un état d'urgence publiquement exprimé et politiquement justifié permettrait de passer outre cette double condition. De telles conditions, qui paraissent à la fois salutaires et minimales, semblent toutefois impossibles à garantir de manière absolue pour la défense des citoyens.

Ensuite, on peut préconiser une ligne de défense dans la relation personnelle aux dispositifs de reconnaissance faciale et biométriques, qui quant à elle paraît susceptible d'être coûte que coûte maintenue : elle concerne, par le biais de l'éducation et de l'auto-éducation aux usages numériques, le refus personnel, toutes les fois que c'est possible, d'accepter l'identification/la personnification biométrique, dans les usages personnels et nonobstant les séductions du marketing des commodités. Ne pas respecter cette ligne reviendrait en effet à accepter de sacrifier les conditions de sa liberté (et en premier lieu, le respect de l'anonymat) à son confort. Formulée en termes arendtiens, une telle attitude consiste à user des ressources de la technologie pour nier son pouvoir d'« action » au profit des conditions de sa « vie ». Ainsi caractérisée, l'acceptation du développement des dispositifs biométrique poursuit de manière contemporaine une tendance typique du modernisme, et elle constitue une tentation très dangereuse[26].

[26] Hannah Arendt, *Condition de l'homme moderne* (1958), chapitre V, trad. G. Fradier, in L'Humaine condition, éd. sous la dir. de Ph. Raynaud, Paris, Gallimard, 2012, p. 294-323.