Des origines de l'identification biométrique à l'intelligence artificielle : la biométrie comme catalyseur des tensions entre sécurité et liberté

Gérard Dubey

▶ **To cite this version:**

Gérard Dubey. Des origines de l'identification biométrique à l'intelligence artificielle : la biométrie comme catalyseur des tensions entre sécurité et liberté. Journal des libertes, 2023, 21, pp.57-74. hal-04607279

HAL Id: hal-04607279
https://hal.science/hal-04607279

Submitted on 12 Jun 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Des origines de l'identification biométrique à l'intelligence artificielle : la biométrie comme catalyseur des tensions entre sécurité et liberté dans la société technologique.

Par Gérard Dubey, professeur de sociologie, Institut-Mines-Telecom Business School/Chercheur au Cetcopra, Université Paris1 Panthéon-Sorbonne.

1. Un champ d'application en extension constante

C'est un bien curieux objet que la biométrie. Etymologiquement, il s'agit bien d'une métrique, une mesure de caractéristiques physiologiques individuelles destinée à discriminer un élément individuel à l'intérieur d'une masse (à partir d'une démarche statistique et pré-algorithmique). C'est la définition la plus simple. Mais l'objet est en réalité protéiforme, labile, insaisissable et la critique semble glisser dessus. Depuis l'époque où j'ai enquêté sur cet objet avec d'autres collègues[1], il y un peu plus d'une quinzaine d'années, ses usages, ses applications ont littéralement explosé. C'est cette prolifération que j'interroge ici, en revenant sur certains des étonnements qui nous avaient saisi à l'époque.

Premier constat donc. Depuis le moment où ont été introduits les premiers éléments biométriques dans les passeports et les visas, ou mises en place par certains établissements scolaires des bornes biométriques d'accès aux cantines, il y a presque une vingtaine d'années, le champ d'application n'a fait que croître : avec une accélération notoire, coextensive aux dernières évolutions de l'intelligence algorithmique (dite à tort IA), de la puissance de calcul des machines et, tout récemment, du renforcement des relations « sans contact » en réponse à la pandémie de covid (avec comme au Japon ou en Corée des applications recourant à la reconnaissance faciale) . Nous pourrions d'ailleurs, au regard de ces premiers éléments, rebaptiser la biométrie « identification bio-numérique ».

Deuxième constat. En face, ou plutôt conjointement aux usages régaliens et sécuritaires qui continuent de se développer et de se perfectionner, les domaines du e-commerce et de l'e-banque constituent le nouvel Eldorado de la biométrie[2]. Des quantités de données d'origine très diverses peuvent désormais être croisées et corrélées pour rendre des services évidemment toujours plus nombreux : Aujourd'hui vous pouvez payer un trajet en train en Chine en utilisant votre visage, à condition d'avoir le feu vert du SCS (le Crédit Social Chinois) ou payer votre déjeuner avec un simple sourire (une filiale d'Alibaba a mis en place le *Smile to Pay* dans les restaurants KFC de Hangzhou). British Airways utilise ce type de dispositif pour faciliter l'embarquement des passagers à l'aéroport d'Heathrow à Londres. Un scan numérique du visage est enregistré lors du passage de la sécurité associé à la carte d'embarquement, ce qui est censé optimiser les flux. Dans l'automobile l'identifiant biométrique est utilisé en remplacement des clés, en domotique pour ouvrir les maisons ou actionner à distance d'autres applications

[1] Sylvie Craipeau, Gérard Dubey, Xavier Guchet, « *Biodev* : du contrôle à distance au macro-système-technique », Rapport finale de recherche, Ministère de l'Intérieur et le Ministère des Affaires Etrangères, Recherche financée par le Conseil de l'Union Européenne, 2006.

[2] Ce qu'on désigne par Néo-banques.

domestiques, en téléphonie mobile pour remplacer les mots de passe[3]. Cette liste est en réalité une liste à la Prévert, ou à la *Bouvard et Pécuchet*.

Il y a presque quelque chose programmatique dans cette expansion. Le simple fait de stocker de plus en plus de données sensibles sur un mobile semble imposer de nouvelles normes de sécurité pour leur accès et leur authentification, et la biométrie alliée à l'IA est la solution toute trouvée. Selon une étude réalisée par MasterCard et l'université d'Oxford, 93% des français étaient favorables à la biométrie pour remplacer les mots de passe. Dans un article paru dans le journal du net daté de 2019 on pouvait lire par exemple que :

> « Habitués dans leur vie quotidienne à être secondés par la technologie, -précise l'article- les utilisateurs ont modifié leurs comportements et leurs attentes. À l'ère du digital et du « tout, tout de suite », il est devenu banal de pouvoir pratiquement tout faire depuis son ordinateur ou son téléphone. Dans un contexte où la notion d'instantanéité des échanges est devenue prépondérante, la vérification des informations du client doit s'industrialiser. Ainsi, pour répondre à ces impératifs de sécurité et de réglementation, l'intelligence artificielle pourrait être la solution »[4].

En tant qu'anthropologue, ce qui m'intéresse est de comprendre le contexte historique, les significations et les pratiques sociales qui confèrent à cette dynamique un caractère presque irrésistible. L'extrait d'article que je viens de citer laisse déjà entrevoir quelques pistes. On comprend par exemple que la prolifération de la biométrie a déjà été préparé par les usages des dispositifs technologiques antérieurs, qu'elle est en quelque sorte justifiée a priori par la pratique quotidienne et familière des grands réseaux numériques. Autrement dit -et c'est ce point de vue que je voudrais faire valoir ici- que si l'obsession sécuritaire et celle du contrôle de la société par les états ou les grandes organisations explique ce « déferlement », ce n'est pas un facteur suffisant. Il y a, dans cet objet, quelque chose qui transcende les frontières entre usages publics et privés, individuels et collectif, bref, qui résiste à la critique et participe d'un imaginaire commun qu'il s'agit de déchiffrer. Avec des différences de style importantes, selon qu'on a affaire à des démocraties libérales ou des régimes autoritaires, des Etats ou des organisations privées, l'identification biométrique se présente comme un catalyseur des tensions et des contradictions qui taraudent les sociétés technologiques. J'entends par là : des sociétés qui délèguent à de grands systèmes techniques et à des automatismes une part de plus en plus importante de ce qui relève normalement d'institutions politiques et sociales, de la liberté de délibérer et de choisir.

S'il y a une chose à retenir pour l'instant de cette profusion, c'est donc :

a. que les progrès de la biométrie sont coextensifs au déploiement des réseaux numériques, et de manière plus substantielle, des communications et des échanges à distance.

b. que si le corps fait son retour au cœur des dispositifs digitaux qui semblaient l'en avoir chassé, c'est de façon paradoxale comme un corps sans chair et sans histoire, essentiellement en contact avec des machines ou des terminaux de lecture.

---

[3] Pour la reconnaissance graphique (graphologie automatisée) voir Nikolas Kairinos., « The integration of biometrics and AI ». *Biometric Technology Today*, Volume 2019, Issue 5, May 2019, Pages 8-10.

[4] https://www.journaldunet.com/solutions/dsi/1424667-comment-l-ia-et-la-biometrie-ont-fait-evoluer-l-identification-a-distance/ .Voir aussi « Le mot de passe aux oubliettes », , 14 septembre *Le monde* 2021.

2. Interroger les lieux communs pour accéder à l'imaginaire social sous-jacent

Je voudrais donc revenir maintenant sur quelques-uns des lieux communs sur lesquels a souvent buté notre recherche un peu pionnière, il y a presque vingt ans.

Il s'agissait d'une enquête réalisée auprès des agents de l'état -policiers aux frontières, et agents consulaires, agents d'ADP - sur l'introduction d'éléments biométriques dans les documents d'identité (passeports) et les badges d'accès aux zones contrôlées; ainsi qu'auprès des enseignants, parents d'élèves, direction et enfants des établissements scolaires ayant introduit cette technique en remplacement de la traditionnelle carte de cantine.Du côté des autorités à l'initiative de ces démarches, la justification était toujours plus ou moins la même : assurer et renforcer la sécurité, en luttant contre la fraude identitaire dans le cadre de l'immigration, en protégeant les enfants contre le vol de cartes. Même si les établissements ayant mis en place ces dispositifs n'étaient pas particulièrement exposés à ce genre de menace.

Du côté des premiers usagers, ce qui nous avait frappé, était la quasi-absence d'images ou de métaphores pour décrire ces techniques. La plupart des réactions se limitaient à quelques lieux communs du type :

- *finalement ce type de reconnaissance a toujours existé* ;

- *c'est pratique*

- *pourquoi s'inquiéter si je n'ai rien à me reprocher* ;

Je vais repartir de ces lieux communs et essayer de les faire parler, en faisant le pari qu'ils en disent long sur l'imaginaire social et les pratiques qui sous-tendent la diffusion de ces techniques. Je laisserai de côté la troisième allégation, par manque de place et parce qu'elle résume en quelque sorte les deux précédentes : une perception locale de ces dispositifs (compris et perçus sur la seule base de l'expérience vécue localement depuis la sphère de l'espace privé) ; une compréhension anhistorique et décontextualisée de la technologie et de la norme (ce qui est objectif n'est pas soumis aux variations du temps).

2.1. Une histoire en trompe-l'œil

Commençons par le premier lieu commun : « *finalement, la biométrie, comme mode de reconnaissance, « ça a toujours existé* ».

Dans un document promotionnel du groupe Thalès, grand fournisseur de solutions biométriques on peut lire :

> « La biométrie répond à une préoccupation très ancienne de prouver son identité, de manière irréfutable, et en utilisant ses différences. Dès la préhistoire, l'homme pressentait que certaines caractéristiques comme la trace de son doigt suffisaient à

l'identifier, et il « signait » de son doigt. Deux siècles avant Jésus Christ, l'empereur Qin Shi authentifiait déjà certains scellés avec une empreinte digitale. » (doc. Thales)[5]

Dans le même ordre d'idées, la biométrie comportementale à vocation prédictive a été comparée à l'antique physiognomonie. Par biométrie comportementale, j'entends les techniques algorithmiques qui permettent de capturer, d'analyser et de croiser un grand nombre de données concernant le comportement d'une personne dans l'objectif d'en dresser le profil ou le pattern. Et parmi ces techniques, figurent de plus en plus d'éléments biométriques comme la reconnaissance vocale, la gestuelle, l'expression des émotions, la signature corporelle (démarche), la façon de taper sur un clavier, de marcher, d'utiliser des objets….autant de traces physiologiques susceptibles d'être saisies par des capteurs et croisées avec d'autres données[6].

La physiognomonie se définit de son côté comme un mode de connaissance qui consiste, pour faire court, à découvrir à partir de l'analyse et de l'interprétation des traits du visage le tempérament et le caractère propre d'un individu. Aux Xème et XIème siècle, Avicenne en faisait un élément essentiel du diagnostic médical. L'étude des traits du visage, rapportés à celle du cosmos (la position des astres), révélait les vices et les vertus responsables du mal et de la guérison, permettait de prédire le comportement de l'individu. Utilisée par l'homme de cour ou le monarque pour démasquer les intentions malveillantes derrière le masque de l'hypocrisie, elle devient une science royale au XVIIème. On la retrouve chez Lavater au XVIIIème siècle et au XIXème siècle sous la figure de l'anthropomorphologie.[7].

Mais en réalité, si l'on y prête un peu attention, l'analogie tourne court. Dans l'identification biométrique actuelle, le corps n'est plus rapporté à un univers de significations (cosmologies) dont il serait la partie visible, mais à un fichier informatique et des bases de données, autrement dit aux capacités d'un dispositif technique sans arrière-plan symbolique. La différence avec les anciennes formes de marquage corporel ou d'identification par le corps saute aux yeux, si je puis dire. Il ne s'agit plus de signes apparents destinés à être vus ou reconnus par d'autres sujets, mais d'informations destinées à être identifiées et traitées par des machines algorithmiques.

C'est l'externalité de cette opération (qui sort de la boucle du contrôle les contrôleurs eux-mêmes, en tant que sujets et interprètes d'un sens à débusquer et à déchiffrer) qui, par sa radicalité, semble nouvelle[8]. L'expression « reconnaissance faciale » (traduction littértale de

[5] https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/inspiration/biometrie. Pour l'histoire de ces techniques voir : Biométrie in Carlo Ginzburg, *Traces, emblèmes et mythes*, /Inde coloniale/Galton p.287; H. Faulds, « On the skin furrows of the hand », dans *Nature*, 28 octobre 1880.

[6] https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/inspiration/biometrie

[7] Vigarello G., *Histoire des pratiques de santé. Le sain et le malsain depuis le moyen-âge.* Paris, Seuil, 1993.

[8] Il s'agit pour simplifier d'identifier un individu à partir de la mesure et du calibrage d'une partie de son corps (pour obtenir un gabarit). Le gabarit obtenu est encodé (il ne s'agit pas d'une image analogique) puis enregistré et stocké dans une base de données informatique. L'identification s'opère par rapprochement automatique entre le gabarit stocké (dans le fichier informatique) et la partie du corps qui lui correspond (à partir d'un terminal de lecture ou lecteur).

l'anglais *Facial Recognition*) ajoute d'ailleurs à la confusion laissant entendre qu'il s'agit bien de reconnaissance alors que le procédé se limite à vérifier et valider la congruence de deux informations codées. Il n'est nul question ici de reconnaissance au sens anthropologique du terme, c'est-à-dire de la façon dont les personnes se connaissent les unes par les autres, par leurs interactions, en ayant recours à leur mémoire, leurs expériences, l'interprétation de traces et de témoignages et, littéralement, co-naissent.
Cette façon de naturaliser l'actuelle biométrie est donc problématique et significative à plus d'un titre. Problématique car elle tend à masquer ce qui pose réellement problème et signale une rupture avec les modalités antérieures d'identification : le problème de l'automaticité du procédé. Une automaticité qui, si l'on n'y prête attention, nous conduit par glissements successifs à faire dériver la norme de faits « objectifs » mesurables et quantifiables. La normativité algorithmique présuppose ainsi une transformation profonde du rapport à la norme qui la rend indifférente au contexte et au temps, indifférente aussi aux humains qui l'interprètent et plus généralement étrangère à la question de la décision humaine[9].

Ce discours est bien sûr celui qui est tenu par les principaux promoteurs, acteurs privés ou Etats, de ces dispositifs. Il s'agit de *storytelling*, comme on dit aujourd'hui, c'est-à-dire de produire un discours qui vise à banaliser, à rendre familiers et inoffensifs de puissants dispositifs de contrôle. Mais il s'agit aussi de bien plus que ce que cette interprétation un peu trop instrumentale laisse entrevoir. L'opération, pour réussir, doit s'appuyer sur un socle de croyances et de valeurs largement partagées, qui la justifient en quelque sorte a priori. Et c'est en cela que le lieu commun est révélateur. Pour « fonctionner », la grille de lecture « naturaliste » de la biométrie s'appuie sur une vision très particulière de la technique, où celle-ci apparait comme indépendante des individus qui la font et des systèmes de valeurs où elle prend naissance. Ce qui prédomine dans cette vision, c'est une forme d'extra-territorialité. La technique tire ici sa légitimité du fait qu'elle serait -un peu sur le modèle idéal de l'Etat- à l'abris des conflits d'intérêts, des valeurs, des passions humaines et des affects, bref, étrangère à tous ce qui caractérise et intéresse la nature humaine.
C'est ce socle invisible de représentations sociales partagées qui intéresse au premier chef l'anthropologue que je suis.

Je ne peux guère aller beaucoup plus loin dans le cadre de cet article. Je mettrai juste en avant cette idée finalement assez simple, mais aux conséquences multiples, que parmi les productions de la culture, la technique est peut-être celle qui semble le plus relever des choses naturelles être les moins sociale, ce qu'elle n'est pas, évidemment[10]. Et cette caractéristique éclaire une tentation assez constante et l'une des grandes ambivalences de la modernité : la tentation d'une technique, ou plutôt d'un fonctionnement automatique, qui nous dispenserait d'avoir à faire des choix, à délibérer, à penser, bref qui nous débarrasserait du fardeau d'être libre. Une telle conception de la technique résonne aussi avec la tentation d'un gouvernement par les nombres

[9] La même interprétation vaut aussi pour cet autre lieu commun : *« Ca n'est pas dangereux pour ceux qui n'ont rien à se reprocher »*. Ici aussi l'individu, à l'image des normes sociales, est pensé comme une réalité immuable et indifférente au changement.

[10] Cet étonnement fut celui de Maurice Halbwachs lorsqu'il remarquait que "de toutes les influences sociales, celles qui prennent la forme d'une technique imitent le mieux le mécanisme des choses non sociales". Halbwachs M., *Les cadres sociaux de la mémoire,* (1925), Paris, Albin Michel, 1994, p.267.

ou par la statistique, cette façon de « gouverner sans gouverner » pour reprendre le titre d'un ouvrage de Thomas Berns[11].

C'est bien cette conception ou cette croyance tacite que l'on retrouve derrière la plupart des arguments qui justifient le recours à la biométrie pour identifier les personnes : le procédé technique, parce que technique et objectif, serait le garant d'un traitement égalitaire, à l'abris des intérêts particuliers et des enjeux de pouvoir, comme de l'erreur humaine. Le fait qu'il n'autorise pas d'interprétation, c'est-à-dire fasse l'économie d'un sujet producteur de sens, n'apparait pas comme un obstacle, mais au contraire comme ce qui le rend légitime.
Ce qui me conduit au deuxième grand lieu commun concernant cet objet.

2.2 . « C'est pratique » ou la question du tiers de confiance:

Cette réplique, très souvent entendue, doit d'abord être prise au premier degré :

- l'identifiant biométrique donne accès au grands réseaux techniques qui structurent les relations sociales et économiques. L'identifiant biométrique, c'est donc un peu comme le badge d'accès, symbole de votre intégration à l'entreprise pour laquelle vous travaillez. De sa possession dépend votre intégration sociale et jusqu'à votre existence sociale (révélé par une femme de ménage d'ADP qui s'inquiétait que ses empreintes, rongées par les produits détergents, ne soient pas lisibles par le lecteur biométrique).

- *« C'est pratique »* signifie que ça peut simplifier la vie en donnant un accès plus direct, rapide et sécurisé (sans risque d'usurpation et de fraude) aux plateformes sur le net et aux services qu'elles rendent. L'identifiant biométrique remplace déjà, sur beaucoup de téléphones, le mot de passe.
  (Je ne serais pas étonné, à vrai dire, qu'on nous le présente très bientôt -si ce n'est pas déjà fait- comme un moyen d'identification parfaitement adapté aux problèmes de la société vieillissante et en proie à toutes les formes de dégénérescence cognitives : La biométrie comme moyen de nous « libérer » du fardeau de la mémoire puisque, selon un dossier consacré à ce thème par *Le Monde*, un internaute possèderait en moyenne jusqu'à 80 identifiants et mots de passe. La biométrie au service du *care* en quelque sorte.)

- « C'est pratique » signifie enfin que l'identifiant biométrique est ce qui permet au système technique de vous reconnaître en tant que personne, pour le service réellement personnalisé que vous attendez de recevoir.

Cette dernière observation débouche sur une première contradiction ou tension :

La recherche d'identifiants censés être résistants aux diverses tentatives de falsification et de fraude, fait écho au jeu débridé des identités qui a cours sur le Net, et au climat de défiance qui

[11] Thomas Berns, *Gouverner sans gouverner. Une archéologie politique de la statistique*. Paris, Puf, 2009. Pour la place prise par la mesure et les nombres dans la gouvernance des sociétés démocratiques, voire notamment : Alain Supiot, *La gouvernance par les nombres*, Paris, Fayard, 2015 ; Olivier Rey, *Quand le monde s'est fait nombre*, Paris, Stock, 2016 et Thierry Ménissier, « Jusqu'où l'institution peut-elle être augmentée ? Pour une éthique publique de l'IA », in « L'intelligence artificielle : raison et magie », *Quaderni*, 105, hiver 2021-2022, pp. 73-89.

en résulte. Je ne pense pas seulement ici aux usurpations d'identités, mais aux possibilités qu'offre le numérique de changer d'identité, de se fabriquer des pseudos ou des avatars autant qu'on en désire.

L'identification biométrique est donc censée assurer l'unité et la continuité de l'identité de la personne à partir de ses caractéristiques physiologiques relativement stables. Mais cela implique de renoncer au jeu avec l'identité dont internet est aujourd'hui le terrain privilégié. Cela entre aussi en conflit avec le principe d'une identité plastique, fondamentalement multiple car sociale, dont le sens change en fonction des contextes et du temps (définition de la personne. En conflit encore avec la conception libérale de l'individu, rétive à toute forme d'assignation.[12]

Ces contradictions ne font pas que révéler la tension entre affirmation des libertés individuelles et besoin de sécurité, inhérente aux sociétés démocratiques, celle dont Alexis de Tocqueville avait bien anticipé les dérives possibles.

- Les interactions qui se développent sur les réseaux numériques -et dont l'identifiant est censé résoudre les risques et les contradictions- valorisent les relations dites *peer to peer*, où est réaffirmé le désir de transactions sans intermédiaires, sans intervention d'un tiers, d'une institution, d'un Etat, qu'on soupçonne toujours d'être incontrôlables[13].

Ce principe du *peer to peer* , repose donc avec acuité la question du tiers de confiance, ou plutôt de sa vacance, dans les réseaux numériques, et plus largement dans les sociétés qui, comme la nôtre, valorisent les relations sans contact, désincarnées.[14]

- Et cela nous renvoie à la façon dont les sociétés modernes se sont, pour le meilleur et pour le pire, très largement pensées et construites autour de grands systèmes techniques, soit d'infrastructures matérielles où circulent des flux constitués indifféremment de choses, d'êtres et de signes et dont la matrice au XIXème est le système ferroviaire[15].

C'est rapporté à ce contexte plus large que l'identifiant biométrique prend tout son sens, non seulement en tant catalyseur des tensions générées par notre façon de penser les rapports

---

[12] Voir par exemple à ce sujet, David Samson, « La biométrie », in *Implications philosophiques*, implications-philosophiques.org/dossiers/sécurité/la-biométrie/2010.

[13] L'identifiant biométrique fait bien ici office, dans les esprits et en promesse, de garant de confiance dans un système *peer to pee*r, un peu comme le fait la cryptologie pour les transactions en bitcoins. Cette réflexion m'est venue à la lecture de Philippe Simonnot, *Nouvelles leçons d'économie contemporaine*, Pris, Gallimard, 1998, pp. 549 à 558.

[14] Gérard Dubey, (2009). «Vers un nouveau contrôle social ? Le cas de l'identification biométrique », *Recherches Sociologiques et Anthropologiques*, novembre, Université de Louvain, Belgique, vol.39, n°2 ; (2008). « Nouvelles techniques d'identification, nouveaux pouvoirs », *Cahiers Internationaux de Sociologie*, vol.CXXV/ 2008/2 ; (2008). « La condition biométrique », *Raisons Politiques*, n° spécial « Sécurité humaine », Paris, Presses de Sciences-Po, 2008/4, n°32

[15] A ce sujet voir notamment : Alain Gras. *Les Macro-Système-Techniques*, Paris, Puf, 1997 ; Thomas Park Hughes, 1983. *Networks of Power-Electrification in Western Society*- Baltimore J.Hopkins Univ.Press, 1983.

sociaux et l'exercice du pouvoir, mais plus profondément, de résoudre le dilemme d'une confiance sans tiers institutionnel pour la garantir. Dans la délégation-transfert à des (automatismes) du soin de nous identifier en tant qu'individus, se joue (rejoue) quelque chose de propre à la civilisation technologique, et qui consiste, comme je viens de le dire, à penser la société à l'image d'une machine qui agirait indépendamment de nous et nous dispenserait d'avoir à nous déterminer comme à devoir faire des choix.

- A l'image du code barre pour la gestion des marchandises, ou du code transpondeur pour les avions de ligne, l'identifiant biométrique est le marqueur des entités vivantes adapté au système d'information et de gestion de flux à partir duquel nous pensons nos interactions avec le monde.
- C'est un moyen d'authentifier de façon prétendument infalsifiable l'individu face à la généralisation des transactions et des échanges à distance, dans un espace anonyme et désincarné non garanti par un tiers de confiance, ou plutôt dans un espace qui s'est précisément construit contre l'idée de tel tiers.

Naturellement l'Etat est toujours en dernier recours ce qui garantit l'identité civile, mais également l'intégrité des infrastructures matérielles sans lesquelles, je l'ai dit, les réseaux numériques et nos interactions soi-disant dématérialisées ne seraient que des vues de l'esprit. Mais un tiers qui refuse de plus en plus de jouer ce rôle. En définitive, le problème posé par la biométrie s'avère donc être coextensif à celui que pose l'intelligence algorithmique : celui d'une confusion grandissante entre la fiabilité de l'expertise algorithmique et les conditions de le confiance. Cela interroge l'adoption massive des systèmes d'IA par les services publics, et son corolaire, le risque nouveau d'une forme « d'autorité des machines »[16].

3. Reproblématiser la biométrie comme phénomène social total : la question du cercle vicieux numérique

Ce qui nous ramène à la critique de ces dispositifs. Je dirai que celle-ci s'est jusqu'à présent surtout attachée à décrypter et dénoncer la biométrie comme moyen de contrôle renforcé au service des états et des grandes organisations. Ce qui est visé principalement par ces critiques est l'utilisation de la singularité comme moyen d'une surveillance généralisée et continue.
Le système de reconnaissance faciale qui alimente le système du crédit social chinois est à cet égard exemplaire et régulièrement mis en avant pour accréditer cette menace sur les libertés individuelles.
Mais cela n'explique pas, ou plutôt ne permet pas de comprendre pourquoi ces technologies se diffusent aussi rapidement dans les démocraties libérales (où elles ont d'ailleurs pris naissance), sous la forme de micro-dispositifs dans des espaces multiples aussi bien publics que privés, commerciaux qu'étatiques.

[16] Voir notamment Thierry Ménissier, « L'IA, un artefact technologique porteur de promesses d'amélioration et riche de zones d'ombre **»,** *Quaderni,* dossier IA, n°105, 2021-2022, p.18. Voir aussi Jean Lassègue, « L'intelligence artificielle, technologie de la vision numérique du monde », in *Cahiers de la justice*, 2019/2 n°2/pp 205-219.

La question que nous adressent les techniques d'IB semble donc déborder l'opposition un peu binaire dans laquelle on a trop tendance à l'enfermer : contrôle étatique contre libertés individuelles, idéologie sécuritaire et pouvoir cannibale contre émancipation individuelle et sociale. Je ne prétends pas que ces prises de consciences et ces actions collectives contre un contrôle social devenu obsessionnel -je pense par exemple aux actions du collectif #Reclaimyourface et de l'observatoire des libertés numériques-ne sont pas importantes. Elles le sont. Mais il me semble tout aussi important et urgent de comprendre les dynamiques qui font que ces formes de contrôle continuent de progresser à un rythme toujours plus soutenu, de repérer quelques-uns de leurs ressorts intimes, ce qui les rend, dans l'imaginaire social et les pratiques, sinon légitimes aux yeux du plus grand nombre, du moins inoffensives et sans problème.

L'autre limite de ces critiques est qu'elles sont toujours plus ou moins intégrées par les industriels du domaine, et techniquement recyclées. Dans un document produit par *Thalès Group* on peut par exemple lire que si :

> « l'identification nécessite en général une base de données centralisée qui permet de comparer les données biométriques de plusieurs personnes, (…) on peut aussi simplement enregistrer des données sur un support décentralisé, du type de nos cartes à microprocesseur. Sur le plan de la protection des données, on privilégiera plutôt un procédé d'authentification avec un support décentralisé. Un tel procédé présente moins de risques. Le support décentralisé est en la possession de l'utilisateur lui-même et ses données ne figurent pas nécessairement dans une base de données. A l'inverse, dans l'hypothèse d'un procédé d'identification nécessitant une base de données externe, l'utilisateur n'a pas la maîtrise physique de ses données, avec tous les risques que cela présente. A partir du moment où les données biométriques sont en possession d'un tiers, il y a toujours un risque qu'elles soient utilisées à des fins différentes de ce à quoi la personne concernée a consenti »[17].

Incidemment, ce document promotionnel pointe l'élément peut-être le plus sensible de ces technologies, ce qui les rend finalement presque naturelles et les justifie à nos yeux, ce que j'ai essayé de formuler autour de la question du tiers de confiance. La question que nous adressent les technologies biométriques pointe en quelque sorte le dilemme des sociétés contemporaines : celui d'interactions directes et sans contact mais sûres, c'est-à-dire dont la confiance serait garantie par le système technique lui-même. Si l'on suit cette logique, le risque de traçabilité ne fait pas que s'accorder avec la revendication des libertés individuelles, il semble paradoxalement en devenir la condition. Le paradoxe est que plus croit le désir d'être reconnu en tant qu'individu singulier dans le grand réseau d'interactions numériques, plus croît le système technique. C'est ce que j'ai appelé récemment, au sujet de la cybersécurité, le « cercle vicieux numérique ». A savoir que pour protéger et garantir contre d'éventuelles intrusions nos transactions sur les réseaux numériques (commerciaux ou étatiques), les opérateurs ont besoin d'acquérir une connaissance de plus en plus précise et fine de ce que vous êtes, de ce que vous

[17] https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/inspiration/biometrie

faites ou comptez faire, autrement dit de tout savoir sur nous en tout lieu et à tout moment[18]. Outre la dépense énergétique que cela engendre, nous devons nous rendre à l'évidence que la mise en péril de la sphère individuelle résulte autant des parades technologiques que nous mettons en place pour la protéger (des cyber-protections comme on les désigne aujourd'hui) que de la malveillance de quelques hackers à la solde d'Etats voyous.

Cette même logique semble œuvrer à la diffusion des techniques d'identification numérique. Comme on peut le lire en introduction du dossier du journal *Le Monde* déjà cité, « la dématérialisation permise par le numérique facilite la tâche des escrocs et rend plus difficile la vérification de l'authenticité d'un document », ce qui justifie la généralisation du recours aux identifiants bio-numériques, censés plus fiables et sûrs. Le caractère tautologique du raisonnement saute aux yeux. Les interactions numériques, à distance et sans contact, facilitent la fraude et érodent la confiance. Pour contrer cette tendance il suffirait d'ajouter aux données existantes d'autres données, biométriques cette fois, mais pas moins numériques, le « bio » jouant curieusement ici le rôle de garant absolu. Le retour du corps, ou plutôt du « bios », au centre de dispositifs censés pouvoir s'en passer, n'est bien sûr qu'un trompe-l'œil. Il s'agit bien, je lai dit, de gabarits, c'est-à-dire toujours et encore de datas et de cartographies numériques.

Ce qui rend la biométrie si intéressante, c'est précisément en ce qu'elle touche aux fondements mêmes de notre rapport à l'institution, à ses impensés. C'est aussi ce qui la rend si difficile à appréhender. La question de l'identifiant biométrique est à la croisé des rapports du politique à la technique, de la norme à l'automatisme, de l'individu à l'institution et de l'institution au corps, à la précarité des individus vivants. Pour comprendre en profondeur ces mutations, il faudrait lire ou relire Pierre Legendre, récemment décédé dans une relative indifférence, qui nous rappelait que l'institution n'a pas pour finalité d'administrer, mais de permettre à des individus chaque jour exposés au « risque » de ne plus être, de continuer à exister, de se tenir debout[19].

Encore un dernier mot pour conclure. Identifier un individu et bientôt le définir à partir de quelques caractéristiques physiologiques ou comportementales convertibles en langage machine représente sans doute la conception la plus pauvre de l'individu qu'on puisse imaginer. L'absence de tiers, comme l'absence de contexte et d'intériorité en font l'équivalent d'une machine et je ne peux pas m'ôter de l'esprit que se comporter en machine, en imiter le fonctionnement, participe d'une brutalisation générale des relations sociales. Mais rassurons-nous. A la « question de savoir si (la machine) est humaine ou pas », Jacques Lacan répondait

[18] « Plusieurs géants de l'industrie ont connu d'importantes violations de données au cours des dernières années. Ces violations de données ont exposé les données vitales de millions de clients. Par conséquent, les entreprises sont constamment à la recherche de meilleures alternatives aux modèles de sécurité traditionnels. Les données biométriques telles que les empreintes digitales et l'iris sont utilisées pour authentifier les employés sur le lieu de travail et identifier les propriétaires de smartphones. Ces données biométriques peuvent être mises en œuvre dans les organisations pour autoriser l'accès aux données confidentielles. La biométrie peut être utilisée avec les mots de passe traditionnels ou les codes PIN pour une authentification multifactorielle. En outre, l'adoption de l'IA contribuera à l'élaboration de protocoles de sécurité axés sur les données. Les systèmes d'IA peuvent minimiser les "erreurs humaines", à condition qu'ils soient correctement programmés et qu'ils contribuent à faire des choix plus rapides grâce à des techniques cognitives ». Abhishek P &al., « An analysis of artificial intelligence in biometrics-the next level of security » *Journal of Critical Reviews* , ISSN- 2394-5125 Vol 7, Issue 1, 2020, pages 571-576

[19] Par exemple : Pierre Legendre, *Leçons VII. Le Désir politique de Dieu. Étude sur les montages de l'État et du droit*, Paris, Fayard, 1988

sans détour : évidemment « elle ne l'est pas ». Avant d'ajouter, « seulement, il s'agit aussi de savoir si l'humain, dans le sens où vous l'entendez, est si humain que ça ».[20]

[20] Jacques Lacan, *Le séminaire,* Paris, Seuil, 1978, livre II, p.367