INSTITUT
POUR QUE L'AVENIR AIT BESOIN DE NOUS
SAPIENS

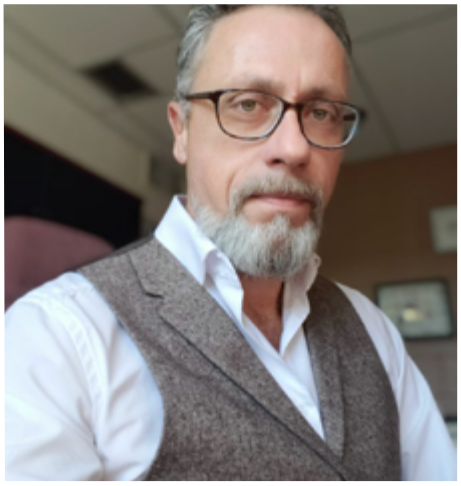
La reconnaissance faciale, faut-il redoubler d'éphores?

Note - Mai 2020

À propos des auteurs

Ysens de France

Docteure en droit public, elle est spécialisée en robotique terrestre. Dans le cadre de son doctorat, elle s'est particulièrement intéressée à l'émergence de systèmes militaires robotisés autonomes dans les conflits armés. Une approche spécifique qui a construit une réflexion prospective et transverse des enjeux liés à l'innovation technologique. Le champ d'application de ses recherches est européen et international, à l'instar de sa collaboration avec euRobotics. Elle est actuellement directrice de la prospective à l'Institut Sapiens.



Emmanuel R. Goffi

Directeur du Centre de recherche et expertise en éthique et intelligence artificielle à l"ILERI – Institut libre d'étude des relations internationales. Il est spécialiste en sciences politiques et éthiques. Il a servi durant 25 ans dans l'armée de l'Air française. Titulaire d'un doctorat en sciences politiques de Science Po Paris, Emmanuel est également professeur en éthique des relations internationales à l'ILERI et chercheur associé au Centre for Defence and Security Studies à la University of Manitoba, à Winnipeg,

Emmanuel a enseigné et conduit des travaux de recherche dans de nombreux établissements universitaires en France et aux Canada. Il intervient régulièrement dans des colloques et dans les médias. Il a publié de nombreux articles et chapitres d'ouvrages et est l'auteur de Les armées françaises face à la moral : une réflexion au cœur des conflits modernes(Paris : L'Harmattan, 2011) et a coordonné un ouvrage de référence sur les drones, Les drones aériens : passé, présent et avenir. Approche globale(Paris: La Documentation française, coll. Stratégie
aérospatiale, 2013).
Ses recherches portent essentiellement sur l'éthique appliquée à la robotique et à l'intelligence artificielle, notamment dans le domaine de la défense.

A propos de l'Institut Sapiens

L'Institut Sapiens est la première « think tech » française. Organisme indépendant à but non lucratif, sa vocation est de peser sur le débat économique et social français par la diffusion de ses idées. Il innove par ses méthodes, son ancrage territorial et la diversité des intervenants qu'il mobilise, afin de mieux penser les enjeux vertigineux du siècle.

Sapiens souhaite défendre la place de l'humain dans une société bouleversée par le numérique. Son axe principal de travail est l'étude et la promotion des nouvelles formes d'écosystèmes favorables au développement économique et au bien-être social.

Sapiens fédère un large réseau d'experts issus de tous horizons, universitaires, avocats, chefs d'entreprise, entrepreneurs, hauts fonctionnaires, autour d'adhérents intéressés par le débat touchant aux grands enjeux actuels.

Plus d'informations sur **http://institutsapiens.fr**

INSTITUT SAPIENS

Introduction

Surveiller les individus et les corriger, dans les deux sens du terme, c'est-à-dire les punir ou les « pédagogiser [1] » est une fonction qui a toujours existé puisqu'elle est le corollaire du maintien de l'ordre social et des formes de pouvoir. En plein cœur du Péloponnèse, à Sparte, un directoire, composé de cinq magistrats élus -les éphores- avait ainsi pour mission le contrôle général de la cité. Avec le dispositif de la reconnaissance faciale, ce sont les modalités mêmes du contrôle exercé par l'État -l'utilisateur final de cette technologie - et par les entreprises -les détenteurs de cette technologie- qui interrogent. S'il est un moyen de sureté et de sécurité nécessaire pour protéger la population[2] , sa généralisation -crainte par l'emploi qui en est déjà fait en Chine ou au Royaume-Uni- interroge non moins les experts juridiques et éthiques que la société toute entière. La demande sans cesse renouvelée de ces mêmes experts d'un moratoire, illustre bien la question sociétale sous-jacente : souhaite-t-on, nous citoyens, que la surveillance « s'exerce au niveau non plus de ce qu'on fait, mais de ce qu'on est, au niveau non de ce qu'on a fait, mais de ce qu'on peut faire? [3] ».

En effet, les dispositifs de surveillance actuels, dont la reconnaissance faciale, se nourrissent des données pour réaliser une cartographie des lieux, des personnes et des activités. Une vision à 360 degrés qui permet de comprendre les habitudes de la population et ainsi ***de déterminer les critères de dangerosité des individus non plus seulement en fonction de leur conduite mais de leur comportement voire de leur personnalité.***

La reconnaissance faciale a ainsi deux applications et deux conséquences. Elle nourrit le profilage en recueillant des données et concourt à leur traitement et donc à caractériser ce profilage. De fait, elle influence la prise de décision finale en ciblant des suspects et transforme le concept politique de « gouvernementalité ». Définie par Foucault, la gouvernementalité est un « ensemble constitué par les institutions, les procédures, analyses et réflexions, les calculs et les tactiques », ayant pour but de « disposer des choses », c'est-à-dire d'obtenir la discipline et l'obéissance de la population sans passer par la contrainte physique [4]et au-delà des normes positives. Un concept auquel Antoinette Rouvroy a apposé le terme algorithmique afin de rendre compte d'une réalité : les

1 Michel Foucault, « Pourquoi le travail social ? », Esprit, n°4-5, avril-mai 1972, p.125.

2 En France, le décret n° 2012-652 du 4 mai 2012 relatif aux traitements d'antécédents judiciaires, permet, dans le cadre d'enquêtes, de coupler des photos de suspect avec une base de données.

3 Michel Foucault, « Conférence, 1974 », repris dans Dits et Écrits (Tome 2), 1970-1975, Paris, Gallimard, 1994.

4 Michel Foucault, Surveiller et punir, Paris, Gallimard, 1975.

systèmes automatiques ont fait du monde physique un objet d'observation, de classification et d'évaluation afin d'agir sur « les possibilités d'action des personnes[5] ». Une transformation silencieuse et durable de la gouvernementalité qui trouve, à travers le terme ***algocatrie***, ses dérives : l'homme devient un document comme les autres[6] » et le gouvernement une plateforme de gestion des algorithmes.

Si nous comprenons l'intérêt sécuritaire d'un dispositif comme la reconnaissance faciale, nous nous questionnons toutefois sur son impact : que pouvons-nous craindre en redoublant d'éphores?[7]

Destinée à devenir une technologie dite intelligente (i.e son fonctionnement est indépendant de toute intervention humaine), son analyse à travers son évolution permet de rappeler qu'elle est le produit d'une convergence technologique[8] (Zoom 1) et l'instrument d'une gouvernance algocratique (Zoom 2).

5 Antoinette ROUVROY « Governmentality in an age of autonomic computing : technology, virtuality, and Utopia », 2011.

6 Olivier ERTZSCHEID, « L'homme, un document comme les autres », Hermès La Revue, CNRS éd., 2009/1, n°53.

7 Nous retrouvons cette formule « redoubler d'éphores » dans le livre de Pierre-Henri Tavoillot , *Comment gouverner un peuple-roi ?* , Ed.Odile Jacob, Paris, 2019.

8 Le concept de convergence technologique rappelle que l'émergence des technologies dites intelligentes est le résultat d'une dynamique à la fois économique, sociétale et technologique. C'est pour cela que la transversalité est au cœur de son étude.

Zoom 1- Identification de la situation actuelle

Techniquement, la reconnaissance faciale n'est pas une nouveauté. Elle s'inscrit dans la volonté de faciliter et transformer l'accès sécurisé à des technologies et des lieux, ainsi en est-il de nos téléphones pour les allumer ou des aéroports pour en sortir. On appelle cela l'identification biométrique, c'est-à-dire la « mesure du corps humain » qui consiste à répondre à la question « qui êtes-vous? ». Dans ce cadre, les données sont avant tout physiologiques (empreintes digitales, forme du visage par exemple). Elles tendent à être couplées à des données comportementales (la gestuelle, le nombre de pas, entre autres). Cette technique d'identification doit être différenciée de celle de l'authentification qui elle, pose la question « êtes-vous bien monsieur X? ». Une interrogation qui soulève celle du modèle de référence biométrique mis en place pour croiser ces données enregistrées avec les caractéristiques de la personne questionnée.

Économiquement, la reconnaissance faciale est une manne financière. Le marché global de la reconnaissance devrait doubler sur la période 2020-2025 pour atteindre 10,2 milliards de dollars[9] . La collecte des données biométriques s'inscrit également dans la course aux données massives (big data) qui nourrissent les systèmes d'IA (notamment dans sa dimension apprentissage – deep learning), et représentent un enjeu économique fort dans un marché très concurrentiel sur lequel la Chine se positionne en leader. En effet, le gouvernement chinois n'a pas les mêmes contraintes culturelles.

Juridiquement, les appels actuels au respect des principes du droit ne concernent pas moins les usages actuels de la reconnaissance faciale (déjà encadrés par le règlement général sur la protection des données (RGPD) et par la directive Police-Justice) que ceux qui seront probablement réalisés s'ils se généralisent. Les inquiétudes liées à cette généralisation naissent du contexte dans lequel cette technologie de l'IA se déploie : la risquophobie de la société qui réclame un droit absolu à sa sécurité et la démagogie technologique qui laisse à penser que chaque utilisateur consent librement à l'utilisation de ses données.

9 Mordor Intelligence, "Facial Recognition Market –Growth, Trends, and Forecast (2020-2025)", January 2020.

• La risquophobie

Le contexte de déploiement de cette technologie est un terreau fertile pour la faire émerger. Comme l'exprimait le secrétaire d'État au numérique, Cédric O, « ce que l'histoire montre, c'est que quand il y a une technologie disponible, à la fin, on finit par l'utiliser ». Une disponibilité à laquelle ni le droit actuel, ni l'éthique, ni le contexte n'offrent de résistance.

En effet, l'utilisation de ces systèmes ne peut actuellement être permise que si elle est justifiée, proportionnée et assortie de garanties adéquates[10] . Il faut, comme l'illustre l'article 10 de la directive Police-Justice un cas de nécessité absolue pour traiter des données biométriques à des fins d'identification. La raison de ces dispositions relevant de cette directive et du RGDP est le respect des droits fondamentaux des personnes. Un garde-fou juridique qui pourrait céder avec le contexte sécuritaire actuel d'une menace diffuse, que la lutte contre le COVID tend à renforcer. Il suffit en effet qu'il y ait un attentat ou qu'une situation soit considérée comme un état de nécessité absolue pour que le gouvernement français décide d'y recourir du jour au lendemain. Là encore, le propos de Cédric O fait écho ***à la nécessité pour le droit de déterminer assez rapidement quelles devront être les circonstances particulières de la mise en œuvre de la reconnaissance faciale à des fins d'identification et d'authentification.*** A défaut de les caractériser, il faudra porter une attention particulière à leurs définitions. Ne nous y trompons pas, cet objectif répond avant tout à un besoin absolu de pédagogie et de formation de notre société et non à un besoin « d'en connaître ». Le drapeau de la transparence numérique, souvent dressée par la population, appelle l'intelligibilité des actions et des décisions prises à l'aide de ces technologies.

Cet objectif à court terme ne doit pas faire oublier le problème de fond. En effet, le risque d'avoir peur et la peur du risque mus par le rejet de l'incertitude et par une culture du « tout technologique », font le lit du développement de ces technologies (qui orienteront nos décisions voire décideront à notre place) et de leur déploiement (elles assainiraient les zones jugées à risque). Les secteurs de l'assurance et du droit sont en première ligne pour proposer de nouvelles offres. Le secteur de l'assurance participera, à travers ses dispositifs de suivi, à appliquer des tarifs sur mesure en fonction de nos comportements (merci les données!). Quant au droit, il devra sans doute évoluer. La proposition de l'Allemagne d'une réglementation sur le risque semble être la seule voie intermédiaire pour encadrer l'essor de cette technologie, plus largement des technologies de l'IA[11] .

10 Commission européenne, Livre blanc. Intelligence artificielle : une approche européenne axée sur l'excellence et la confiance, COM(2020) 65 final, Bruxelles, 19 février 2020, p. 25.

11 Ibidem

• La démagogie technologique

La reconnaissance faciale est une technologie qui, même si elle n'est pas totalement aboutie, laisse entrevoir tout son potentiel. Son déploiement massif sur de multiples supports participe à son évolution vers des applications capables d'impacter radicalement la décision humaine. En effet, la promesse d'un accès plus sécurisé à un espace donné (virtuel ou physique) doit se mesurer à l'aune de la capacité à maîtriser et à suivre sa trace numérique. Où est stocké notre visage virtuel et quelles sont les finalités de sa collecte et de son traitement?

L'avenir de ces données physiologiques est un enjeu clé de la réflexion sur les modalités d'exploitation de la reconnaissance faciale. La raison est l'influence que leur traitement aura sur la décision humaine. S'il est demandé ***le consentement individuel pour le stockage et le traitement de ces données, il n'est en revanche pas certain que celui-ci soit éclairé.*** Ainsi, comme le rappelle Patrick Valduriez, « [l]es messages d'internautes qui disent «je n'autorise pas Facebook à utiliser mes données personnelles» n'ont aucune valeur juridique. Si vous utilisez Facebook, vous acceptez que l'entreprise utilise vos informations comme elle le souhaite ». La réalité c'est que ces informations sont reléguées à des mentions légales peu lues et souvent inintelligibles. Si l'excès de confiance en la technologie affaiblit son contrôle, une méfiance abusive en son usage suscite des fantasmes.

Dans l'incertitude technologique, toute la difficulté pour le droit est de trouver ce point d'équilibre entre rejet qui emporte son interdiction et acceptation qui emporte des dérives.

Zoom 2 - La mise en place d'une algocratie, une situation à craindre

La mise en place de la société de surveillance procède du postulat de l'existence d'une menace elle-même produite par l'idée que nous sommes des suspects, coupables en devenir qu'il convient de discipliner. C'est le sujet même de *Minority Report*. Cette notion de menace justifie et légitime le recours à des critères juridiques et éthiques pour épingler l'homme suspect et standardiser les comportements.

• L'homme suspect

L'émergence de nouvelles technologies convoque sans arrêt le droit pour répondre aux risques d'irrespect que leur déploiement sous-tend.

Un droit qui peine à trouver des réponses adéquates en raison d'un défaut de maturité de ces technologies. En effet, sans critères techniques fiables il ne peut y avoir de critères juridiques stables.

La reconnaissance faciale vient fait naitre un droit qui tend de plus en plus à programmer plutôt qu'à légiférer. Ce constat avait été déjà soulevé par Lawrence Lessig lorsqu'il évoquait le *« code is law ».* Ainsi, avec la reconnaissance faciale, on assiste à l'évolution d'un droit qui ne sanctionne plus seulement des conduites illégales mais oriente des comportements, préfigurant alors le fichage de modèles de personnalités jugés à risques. Du modèle préventif très souvent contesté, on glisserait vers un ***modèle prescriptif.*** Une sorte de nouvelle Pythie, oracle moderne générateur de prophéties auto-réalisatrices, marchande de sécurité au prix de l'abolition des libertés individuelles, qui arguant de l'existence d'une menace permanente justifie et légitime la surveillance permanente.

Nous pourrions alors craindre le sacrifice sur l'autel de l'efficacité du concept d'équité qui est aux principes de nos systèmes juridiques. La présomption d'innocence[12] pourrait s'en trouver transformée, sans mot dire, en une présomption de culpabilité tout comme l'obligation de déterminer le lien de causalité entre une action et la personne pourrait se transformer en lien de corrélation entre un contexte et une personnalité. Il faut craindre également le passage de la transgression des règles sociales à celle de la réaction émotionnelle inadaptée. Ce qui emporte un risque de standardisation des comportements qui amène à craindre l'émergence du crédit social à la chinoise.

Cela nous amène à notre deuxième inquiétude, le changement de paradigme de la société.

• La gouvernance technologique

Le déploiement de la reconnaissance faciale n'est pas sans rappeler la mise en place théorique du Panoptique de Bentham[13] . Il théorise la société de surveillance à travers l'image d'une prison dont les cellules sont grillagées et plongent sur une cour intérieure qui trouve en son centre une tour de contrôle où des surveillants peuvent voir sans être vus. Il faut, dit-il, imaginer « l'ensemble de cet édifice comme une ruche dont chaque cellule est visible d'un point central. L'inspecteur invisible lui-même règne comme un esprit, mais cet esprit peut au besoin donner immédiatement la preuve d'une présence réelle[14] ». La question ici n'est

12 Contrairement à ce qui est souvent sous-entendu dans l'opinion publique, tout homme est présumé innocent jusqu'à ce qu'il ait été déclaré coupable (article 9 de la Déclaration des droits de l'homme et du citoyen du 26 aout 1789).

13 Idée des frères Bentham, formulée par Jérémy BENTHAM, Panoptique Mémoire sur un nouveau principe pour construire des maisons d'inspection et nommément des maisons de force, 1791.

14 Ibidem.

pas moins de remettre en cause la société de contrôle que les nouvelles modalités de fonctionnement qui emportent des conséquences :

L'inquiétude de ***la réduction de l'humain à une équation mathématique.*** Il est « mathématisé », réduit au rang d'automate, de suites de chiffres donnant naissance à des probabilités. Rationnalisé à l'excès, l'humain est déshumanisé. La logique mathématicienne est développée jusqu'à désigner la réalité elle-même et permettre le développement de concepts inappropriées comme l'éthique universelle…

L'inquiétude également de ***la réduction de l'autorité de l'État.*** Paradoxalement et comme le soulignait Gilles Deleuze, après la société disciplinaire dans laquelle la surveillance est centralisée et réciproque (dite panoptique) vient la surveillance décentralisée et réciproque (dit rhizomique). Le concept d'État plateforme prendrait alors tout son sens en tant que « monstre froid[15] » dont la marche est commandée par des processus automatiques et gérée par des opérateurs privés (le célèbre *Little brother is watching you*) . Il pourrait en ressortir, une crise de confiance encore plus importante de la population envers son gouvernement, faisant dériver l'idéal technologique d'une société de confiance vers une société de méfiance délétère.

Zoom 3- Des recommandations

Londres, Madrid et bientôt Paris? Le dispositif de la reconnaissance faciale à des fins d'identification semble se déployer sur le continent européen. L'application numérique de suivi des confinés est une pierre de plus posée à l'effigie de technologies avancées qui sauvent notre monde du chaos sécuritaire… Sans doute, a-t-on besoin de ces expérimentations pour permettre à la société de comprendre et de voir ce qui déroule sous ses yeux. Il faut l'espérer car, elle a surtout clairement démontré jusqu'à aujourd'hui, qu'au nom du risque, la technologie pouvait servir d'anesthésiant populaire.

A l'instar de l'UE, nous pensons que cette technologie doit s'entourer d'exigences spécifiques lorsqu'elle permet l'identification des individus. Des exigences qui doivent être formulées à l'aune d'une des probables dérives, l'authentification. La Chine, bien que disposant d'une culture holistique très différente de celle de l'Europe, individualiste, illustre ce risque et éclaire nos recommandations.

1- Créer des Eyes Boxes, des zones d'expérimentation pour déterminer les cas d'usage. Une expérimentation qui devra être réalisée par des entreprises françaises car se joue, en creux, la souveraineté numérique de la France.

15 Virginie TOURNAY, Le Monde, 22 novembre 2017.

2- Garantir le droit à la connaissance à chacun porté par l'article 9 alinéa 1 de la Convention dit « 108 + ». En vertu de son alinéa C, celles-ci ont le droit d'obtenir connaissance du raisonnement qui sous-tend le traitement des données, y compris les conséquences de ce raisonnement et les conclusions qui peuvent en avoir été tirées, en particulier lors de l'utilisation d'algorithmes pour une prise de décision automatisée, notamment dans le cadre du profilage ».

3- Réaliser un moratoire populaire à défaut d'une décision politique claire sur cette question. Si ce moratoire est révélateur de l'enjeu de société inhérent à ce dispositif il démontre également la défaillance de l'autorité politique à décider dans l'incertitude technologique.

4- Assumer la visée éthique téléologique et cesser de manipuler les perceptions en recourant à des concepts bienpensants et superficiels.

5- Nourrir et faire avancer les réflexions juridiques concernant une ***réglementation sur le risque.*** L'innovation de cette réglementation réside dans son classement à plusieurs niveaux, en fonction à la fois de la nature de la technologie, de son secteur d'utilisation et de ses potentiels dérives (au regard de son accessibilité et de sa réversibilité). Cette réglementation concerne toutes les technologies d'IA, qu'elles soient robotisées (utilisation de l'IA dans un corps mécanisé) ou non (le cas de la caméra de surveillance intelligente).