Inhaltsverzeichnis / Table des matières

Visages en otage : audaces et périls des technologies de reconnaissance faciale en prévention du crime

Manon Jendly*

Table des matières

Résumé

Le recours croissant par les autorités policières aux technologies de reconnaissance faciale (TRF) à des fins préventives cristallise à la fois des promesses et des périls. Alors qu'elles font l'objet de vives controverses, ces technologies connaissent un essor fulgurant dans de nombreux pays et la question de leur déploiement plus large et toujours plus automatisé pourrait se poser à terme en Suisse également. Dans cette contribution, il est question des TRF utilisées à titre d'identification à distance et en temps réel dans les espaces publics. Nous en brossons d'abord les principaux enjeux, à partir de quelques exemples tirés de leur exploitation aux Etats-Unis et de leurs récentes expérimentations en Europe. Nous questionnons ensuite les timides limites destinées à encadrer leurs audaces et le faible niveau de connaissance relatif à leurs (més)usages. Nous soulignons enfin les principales questions susceptibles de diligenter notre réflexion les entourant,

* Professeure associée, Ecole des sciences criminelles, Université de Lausanne.

dans un contexte plus général de recueil massif de données sur nos personnes pour des motifs dits de sécurité.

Zusammenfassung

Der zunehmende Einsatz von Gesichtserkennungstechnologien (*Facial recognition technologies*, FRT) durch die Polizei zu präventiven Zwecken birgt sowohl Versprechen als auch Gefahren. Obwohl sie Gegenstand heftiger Kontroversen sind, erfahren diese Technologien in vielen Ländern eine rasante Entwicklung, und die Frage nach ihrem umfassenden und zunehmend automatisierteren Einsatz könnte sich schliesslich auch in der Schweiz stellen. In diesem Beitrag geht es um FRTs, die zur Fern- und Echtzeitidentifikation im öffentlichen Raum verwendet werden. Wir skizzieren zunächst die Hauptprobleme anhand einiger Beispiele aus ihrem Einsatz in den Vereinigten Staaten und ihren jüngsten Experimenten in Europa. Dann hinterfragen wir die zaghaften Versuche, diesen Systemen Grenzen zu setzen, die ihren Einsatz einrahmen, ebenso wie das geringe Wissen über deren Einsatz- und Missbrauchsmöglichkeiten. Schliesslich geht es um die wichtigen Fragen, die unser Denken in Bezug auf sie wahrscheinlich weiter verfeinern werden, in einem allgemeineren Kontext der massiven Sammlung von Daten über Personen aus sogenannten Sicherheitsgründen.

1. Introduction

C'est à l'occasion d'un séjour d'une année à Los Angeles, en 2019, que j'ai été sérieusement interpellée par l'omniprésence, dans mes activités routinières, de différents dispositifs de reconnaissance faciale. Ainsi m'était-il proposé, le matin de bonne heure, de lier mon visage à un porte-monnaie électronique pour accéder à une tasse de café. En emmenant les enfants à l'école publique, il était discuté entre parents de la pertinence de déployer ces dispositifs pour contrôler les entrées dans la cour. Lors de patrouilles avec la police de Los Angeles (LAPD), j'étais témoin de vives discussions entre les agents sur l'opportunité de les conjuguer à leur *bodycam*. Enfin, en soirée, je m'y confrontais encore à l'occasion d'un concert de Taylor Swift au Rose Bowl Stadium, dont les équipes de sécurité utilisaient cette technologie pour identifier en temps réel, dans la foule, certains admirateurs compulsifs de la star.

Il existe une pluralité de technologies de reconnaissance faciale (ci-après «TRF»), allant des systèmes se bornant à détecter la présence d'un visage sur une image, à ceux qui visent à identifier un individu unique en confrontant une image de visage captée par une caméra de vidéosurveillance à un set de visages compris dans une base de données (Buolamwini *et al.*, 2020). Ces technologies pénètrent un nombre croissant de secteurs d'activités et

représentent une industrie vertigineuse : les analystes estiment leur taux de croissance annuelle entre 15 % et 20 %, pour atteindre près de 10 milliards de dollars de recettes en 2022[1], un montant revu récemment à la hausse en raison des nouveaux dispositifs développés pour juguler les risques sanitaires en temps de Covid-19 (Yan, 2020). Ces technologies ont investi le milieu scolaire, au motif qu'elles pourraient aider à neutraliser les personnes non autorisées dans les préaux, faciliter l'enregistrement des présences en classe des élèves et enseignants, ou encore mesurer leur degré d'attention mutuelle. Il y est recouru en milieu professionnel, lors de processus de recrutement, pour analyser les expressions faciales des candidat.e.s, présumément de sorte à révéler leurs principaux traits de caractère[2]. Les commerces également s'en dotent pour vérifier l'identité et l'âge de leurs clients concernant certaines consommations, faciliter leurs paiements, lier leurs déplacements à leurs habitudes de consommation et prévenir les vols. Elles sont mobilisées lors des contrôles aux frontières pour assurer leur protection contre toute immixtion réputée illégale ou pour accélérer les flux, en remplacement des contrôles manuels de passeports et cartes d'embarquement. Ces technologies font aussi l'objet d'une utilisation accrue par la police, dans le cadre d'enquêtes, afin d'identifier des suspects, et toujours plus à des fins de prévention de la criminalité, en particulier lorsqu'elles sont déployées lors de certains événements sportifs et culturels ou plus subrepticement conjuguées aux *bodycams* ou aux caméras de vidéosurveillance dans les espaces accessibles au public (Blount, 2017). Les pratiques de collecte et d'analyse d'images de visages semblent donc progressivement se profiler comme un moyen privilégié destiné à juguler les incertitudes modernes, qu'elles concernent nos relations et interactions personnelles, amoureuses et professionnelles, nos habitudes de consommation, nos mobilités et, plus généralement, nos propensions à adopter ou non une vie conventionnelle.

En tant que telle, la reconnaissance des visages sous forme informatique remonte aux travaux de Woodrow Bledsoe et de son équipe dans les années 1960 (Raviv, 2020). Ses développements gagnent progressivement en puissance au fil des années et, s'agissant de ses applications dans le domaine du main-

1 Pour des précisions sur ces prévisions, voir ‹https://www.grandviewresearch.com/industry-analysis/facial-recognition-market› et ‹https://www.marketresearchfuture.com/reports/facial-recognition-market-1250› (tous deux consultés le 21.4.21).

2 La reconnaissance affective (affective recognition) constitue un sous-ensemble de la reconnaissance faciale, qui tente d'identifier les (micro-)expressions et émotions d'individus à partir d'images de leurs visages (photographies ou vidéos). Whittaker *et al.* (2018, 14) établissent un lien entre la reconnaissance affective et la physiognomie, « une pseudoscience qui prétend que les traits du visage peuvent révéler des aspects innés de notre caractère ou de notre personnalité », largement décriée pour sa propension à perpétuer des stéréotypes fondés notamment sur le genre ou la race. Dans le même sens, Agüera y Arcas *et al.* (2017) étayent les dérapages et mythologies des différentes démarches, y compris celles relevant des techniques d'apprentissage machine, vouées à déceler par inférence faciale les « figures du mal ».

tien de l'ordre et de la sécurité, sous la conjonction de plusieurs facteurs. Le premier ressort est étroitement lié aux actualités. Les événements du 11 septembre 2001 en particulier ont été jalonnés de nombreux appels à développer massivement ce type de technologie et à y recourir dans la « *Global War on Terror* » lancée à leur issue (Gates, 2011). De fait, en 2016 déjà, un adulte américain sur deux avait sa photo dans une base de données de reconnaissance faciale des forces de l'ordre aux Etats-Unis, pour près de 641 millions d'images de visages au total (Georgetown Law Center on Privacy and Technology, 2016). Le deuxième facteur a trait aux évolutions techno-scientifiques, s'agissant en particulier de la correspondance biométrique, de l'analyse computationnelle des *Big data* et de l'intelligence artificielle dite forte, de type *deep learning* (apprentissage profond), ces trois éléments se renforçant mutuellement dans un contexte saturé d'une puissante rhétorique soutenant la collecte et l'exploitation des données pour anticiper les risques, le plus souvent inhérents aux activités humaines. Le troisième élément, enfin, est d'ordre plus organisationnel. Il découle d'une division du travail toujours plus morcelée dans le champ de la sécurité et du renseignement, dans lequel se multiplient les partenariats publics-privés entre les préposés étatiques à la sécurité publique et les développeurs des technologies dites « *data-driven* » ou « *data-led* », et plus récemment qualifiées de « *smart* » (Biometrics and Forensics Ethics Group, 2021). Les traditionnels acteurs étatiques de la sécurité s'équipent, en effet, désormais assez aisément en appareillages développés par des entreprises privées, qui louent leurs atouts pour créer « un monde plus sûr », comme aime à le souligner notamment Peter Trepp, CEO de la start-up californienne *Facefirst*[3], qui figure parmi les leaders du marché des TRF.

Je propose, dans cette contribution, de tempérer fortement cette assertion, selon laquelle les TRF participeraient à un « monde plus sûr », à partir d'un bref panorama des implications sociales et politiques de ces technologies. Elles constituent en effet un cas d'application plutôt révélateur des enjeux entourant les dispositifs de recueil d'informations sur nos personnes au motif d'une « sécurité » dont la définition et les moyens activés pour y parvenir ne font pas consensus. Comme toute autre technologie de pouvoir, elles n'ont pas pour objectif de s'attaquer aux causes structurelles entourant le crime et la déviance, mais plus de gérer leurs symptômes, sous couvert d'efficacité, de neutralité et d'efficience présumées (Smith, 2020). Plus spécifiquement, ces technologies cristallisent la place, désormais centrale, qu'occupent les images de visages humains dans la constellation des politiques, des pratiques et des acteurs impliqués dans le raffinage d'un *certain* modèle de régulation sociale (Introna et Wood, 2004). Fondé sur la collecte massive et l'analyse de données

3 Ainsi s'exprimait-t-il dans la version de 2020 du site internet de l'entreprise : « *FaceFirst's face recognition system is creating a safer planet through face recognition security software for retailers, airports, law enforcement and more* ».

à caractère personnel, ce modèle poursuit un idéal de connaissance toujours plus précise et perfectionnée de chaque individu pris pour lui seul, de sorte à l'affilier à une catégorie d'accès, de privilège ou encore de risque, qui peut sérieusement impacter son existence (Hannah-Moffat, 2019). Ce modèle renverse les pouvoirs en présence : Là où l'Etat disposait auparavant du monopole de l'arbitrage, les pourvoyeurs desdites technologies arrêtent maintenant les règles du jeu. Ces règles sont celles d'un marché très concurrentiel et qui louvoie sérieusement avec tout contrôle étatique, quand bien même il est question ici de données biométriques. Partant, cette contribution s'articule en 4 parties. La première s'attache à présenter brièvement les contours des TRF et les deux tâches les plus courantes qui leur sont associées. La deuxième traite plus spécifiquement d'un cas d'application de l'une d'elle, l'identification, déployée par certaines polices à distance et en temps réel dans les espaces publics. Les principaux enjeux liés à ces technologies sont brièvement présentés dans la troisième partie. Enfin, on se posera la question de savoir quelles sont les représentations de ces dispositifs au sein de la société civile, pour mieux souligner l'importance de demeurer vigilant, au risque sinon de participer à l'avènement d'une « *corporate surveillance* » générale et généralisée, dissimulée sous l'évocation fallacieuse d'un « *safer world* ».

2. Modalités des (L)TRF

Dans sa version la plus récente, la reconnaissance faciale est un processus automatisé qui consiste à repérer puis comparer une image de visage avec d'autres pour déterminer si elles représentent le même individu[4]. La première étape de ce processus consiste en la détection d'un visage. Elle implique qu'un algorithme repère le visage d'une personne, soit en scannant une image qui lui est soumise, soit en fouillant dans un amas de photos ou de vidéos déjà constitué. Une fois détecté, le visage est « normalisé », mis à l'échelle et aligné de sorte que l'algorithme puisse en extraire des caractéristiques qui peuvent être quantifiées numériquement, comme la position et la distance entre les yeux ou l'écart entre le menton et le front. Ensuite, l'algorithme paire le visage avec d'autres visages, tirés d'une ou plusieurs autres sources, et émet un score reflétant la similitude de leurs caractéristiques. C'est ce qu'on appelle la comparaison/classification. La dernière étape, enfin, étant celle de l'éventuel « *matching* », à savoir la reconnaissance en tant que telle (Garvie *et al.*, 2016).

Deux des tâches désormais les plus courantes de la reconnaissance faciale sont l'authentification (*face verification*) et l'identification (*face identification*). Dans les deux cas, la reconnaissance des visages repose sur une estimation de

4 Pour des précisions relatives aux différents modèles algorithmiques diligentant les systèmes automatiques, voir Jacquet/Grossrieder (2021).

correspondance de type probabiliste. Elle ne produit pas de réponses binaires « oui » ou « non », mais une probabilité que la personne est bien celle que l'on cherche à authentifier ou à identifier. Si cette probabilité dépasse un seuil déterminé dans le système, alors ce dernier considère qu'il y a correspondance (CNIL, 2019).

L'*authentification* consiste à vérifier la correspondance entre le visage d'une personne à l'image d'un visage de référence de cette même personne, contenue par exemple dans une base de données. On vérifie donc ici si le visage mis à l'épreuve correspond bien à l'image préenregistrée. On parle de comparaison 1 : 1 ou de « *1-to-1 matching* ». Il est donc question d'authentification quand on utilise la reconnaissance faciale pour déverrouiller son *smart*phone, retirer de l'argent, ou encore quand est utilisée, à l'aéroport de Zurich depuis 2017 ou celui de Genève depuis la fin 2019, une borne de contrôle par reconnaissance faciale automatisée pour vérifier les papiers d'identité des usagers.

L'*identification*, en revanche, consiste à déterminer si le visage d'une personne a une correspondance avec une ou plusieurs autres images de visages comprises dans une ou plusieurs bases de données de « personnes d'intérêt », parfois appelées « *gallery* ». On parle alors de recherche « un-à-plusieurs » ou « *1-to-many matching* ». Cette méthode est utilisée par la police notamment pour identifier des suspects dans le cadre d'une enquête, à travers des bases de données gouvernementales, par exemple de photos d'identité judiciaire. C'est le cas d'Interpol, qui avance avoir identifié plus de 1000 criminels, fugitifs et personnes disparues depuis le lancement de son système de reconnaissance faciale IFRS en 2016, comprenant des images de visages communiquées par plus de 179 pays[5].

Plus récemment, avec les avancées technologiques, la tendance est d'opérer à distance et en temps réel l'identification de personnes dans les espaces publics *(Live Facial Recognition,* abrégée ci-après LTRF), à l'appui de « liste(s) de surveillance ». C'est ce qu'expérimente la police métropolitaine de Londres (MET), par exemple, au motif que cette technologie sera, à terme, « un outil efficace de lutte contre la criminalité, offrant davantage de possibilités d'arrêter les délinquants violents, d'arrêter les terroristes en puissance et de protéger les personnes les plus vulnérables de la société » (Metropolitan police, 2020, 11, trad. libre). Concrètement, des caméras de reconnaissance sont déployées sur un périmètre. Elles détectent et scannent les visages des personnes qui passent dans cette zone et transmettent directement ces images au système de reconnaissance faciale en direct *NeoFace* de l'entreprise NEC. Ce système contient une « *watch list* », comprenant les visages de délinquants recherchés par la police ou les tribunaux et d'autres personnes présumées présenter un

5 Voir ‹https://www.interpol.int/fr/Notre-action/Police-scientifique/Reconnaissance-faciale› (consulté le 21.4.21).

risque de préjudice pour elles-mêmes ou pour autrui. L'algorithme extrait les caractéristiques et calcule la structure de chaque visage pour créer un modèle facial. Les visages sont alors comparés aux images des personnes figurant sur la liste de surveillance, élaborée notamment sur la base de données d'images de visages de la MET, mais également d'autres sources plus controversées (The Law Society of England and Wales, 2019). Si l'algorithme trouve une correspondance, il envoie une alerte aux agents présents sur les lieux. Un agent compare alors le visage de l'alerte à la personne qu'il voit sur site et décide ou non d'intervenir. Dans le cas présent, le système ne conserve que les images qui ont généré une alerte, pendant 31 jours maximum ou, en cas d'arrestation, jusqu'à la fin de l'enquête ou de la procédure judiciaire. Celles qui n'ont pas donné lieu à une alerte sont apparemment automatiquement et immédiatement effacées (Fussey *et al.*, 2019 ; Bradford *et al.*, 2020). Ce dispositif a fait l'objet de nombreuses critiques (London Policing Ethics Panel, 2018 et 2019 ; Wiles, 2019 et 2020). L'usage d'un dispositif similaire par la police du sud du Pays de Galle a même fait l'objet d'une décision judiciaire de la Cour d'appel estimant son utilisation contraire à l'art. 8 CEDH[6]. Il n'empêche, les initiatives se multiplient toutefois pour poursuivre les expérimentations (Biometrics and Forensics Ethics Group, 2021).

3. De quelques enjeux

Contrairement aux autres technologies qui exploitent des données biométriques, par exemple des empreintes digitales, les LTFR peuvent être déployées à distance et à la volée, c'est-à-dire indistinctement et potentiellement en toute ignorance des personnes visées. Les systèmes de reconnaissance faciale en temps réel suscitent donc des questions épineuses en termes éthiques et juridiques, s'agissant notamment du droit au consentement, à l'autodétermination et à l'anonymat dans les espaces publics. Au-delà, elles révèlent avec une acuité particulière les implications sociétales, voire les compromis politiques, entourant des actions de prévention du crime toujours plus souvent fondées sur le recueil massif de données et des technologies diligentées par des algorithmes d'apprentissage destinés à les « faire parler ». A date, ce sont leurs enjeux techniques et légaux qui sont les mieux documentés. L'exploitation de ces technologies dans les activités dites « de sécurité et de maintien de l'ordre » suscite toutefois aussi de nombreuses questions, notamment en termes de gouvernance, de surveillance et de connaissance, qui en appellent à un débat plus démocratique sur leur écosystème[7].

6 Voir R (Bridges) v. Chief Constable of South Wales Police ([2020] EWCA Civ 1058), décision sur appel du 11.8.2020.

7 Sur les enjeux d'appropriation, dont il ne sera pas ici question, voir Fussey *et al.* (2021).

3.1 Enjeux techno-politiques

Les expérimentations réalisées jusqu'à présent sur le recours aux LTRF démontrent qu'elles mènent à des résultats mitigés, voire à des erreurs. A titre d'exemple, une analyse indépendante de six périodes d'essai du système de la Police métropolitaine de Londres entre 2018 et 2019 rend compte que, sur 46 alertes générées par le logiciel, et les 42 retenues pour analyse, seules huit correspondances de reconnaissance faciale ont pu être validées, ce qui signifie que le dispositif n'a abouti que dans 19 % des cas (Fussey/Murray, 2019). Plus grave, les algorithmes de reconnaissance faciale peuvent perpétuer des biais fondés sur des caractéristiques démographiques. Le dernier rapport d'évaluation du *National Institute of Standards and Technology* américain est, à cet égard, particulièrement révélateur (Grother *et al.*, 2019). Il rend compte de la performance d'authentification et d'identification de 189 algorithmes de reconnaissance faciale, développés par 99 acteurs influents du domaine. Ces algorithmes sont testés à l'appui de quatre bases de données de visages, détenues notamment par le *Department of Homeland Security* et le *FBI*, totalisant plus de 18 millions de visages couvrant plus de 8 millions de personnes. Ces collections de visages incluent également des informations sur l'âge, le sexe, la race et/ou le pays d'origine des sujets. Les chercheurs ont mesuré les faux résultats positifs et les faux résultats négatifs de chaque algorithme pour les deux types de tâches. Les résultats les plus interpellants concernent les taux de faux résultats positifs qui révèlent des biais de race, de genre et d'âge. Ainsi, pour les appariements « *1-to-many* » qui nous intéressent, les chercheurs observent des taux significativement plus élevés de faux résultats positifs chez les femmes afro-descendantes.

Ces erreurs et ces biais sont notamment liés au fait que les processus, les métriques, les sets de données sur lesquels ces technologies sont entrainées (ou s'entrainent seules) et/ou leurs conditions d'expérimentation reflètent des choix de société, qui ne sont ni neutres ni impartiaux (Mohamed *et al.*, 2020). Le design retenu, le peu de diversité parmi leurs développeurs, ou encore la nature et la qualité des données sont parmi les dimensions qui façonnent ces technologies (Buolamwini/Gebru, 2018 ; Garvie, 2019 ; Hooker, 2021). Socialement et culturellement situées, les (L)TRF reflètent une certaine conception du monde et relaient des référentiels dominants (Cardon, 2015).

Leurs modalités et leur contexte d'utilisation importent également, dès lors qu'ils charrient, eux aussi, de tels choix. Tel est le cas lorsqu'il y est recouru de manière disproportionnée sur certaines communautés ou lorsqu'elles sont conjuguées à des listes de personnes d'intérêt faisandées *ab initio*, typiquement dans un contexte de lutte dure contre le terrorisme (Fussey/Murray, 2019). S'attaquer aux biais en portant une attention particulière à la nature des données d'entrainement (« *data pipeline* ») ne suffit donc pas, pis peut avoir les effets contraires de ceux escomptés. Par exemple, c'est en évoquant l'argu-

ment de la nécessité d'offrir à ses ingénieurs « une meilleure diversité de tons de peau » que l'entreprise IBM a obtenu de la police de Manhattan (NYPD) qu'elle les laisse accéder à toutes ses caméras de la basse île. Son logiciel ainsi perfectionné a été exploité ensuite pour identifier à distance des profils affiliés à « la menace », renforçant de graves amalgames fondés sur la couleur de la peau et/ou sur l'origine présumée (Joseph/Lipp, 2018). En ciblant ainsi la « correction technique » sous prétexte d'une quête de neutralité et d'équité, le débat politique entourant le développement et le recours à ces dispositifs, les valeurs et le projet de société qu'elles charrient, bien que crucial, est subtilement éludé (Crawford, 2021).

3.2 Enjeux juridiques

En Amérique du Nord, ces technologies ont été prohibées ou suspendues là même où elles ont, pour partie, été développées. A San Francisco par exemple, il est désormais interdit à la police d'y recourir à la suite de l'adoption par la municipalité de l'ordonnance « *Stop Surveillance* ». Au-delà de leurs déficits « techniques », les raisons pour suspendre l'utilisation de ces technologies sont nombreuses : il est ainsi évoqué la protection de la vie privée et des données sensibles, le droit de se réunir et de manifester, comme le droit à un procès équitable, *e.g.* celui de pouvoir se déterminer en toute connaissance de cause sur les preuves à charge, lesquelles ne peuvent être discutées si le code de l'algorithme de reconnaissance est tenu secret. On relève également les impacts disparates de ces technologies, susceptibles de mener à des inégalités de traitement fondées sur l'identité de genre, l'âge, la couleur de peau, l'origine ou encore le handicap. La question est d'ailleurs érigée en priorité par les défenseurs des droits civils qui en appellent à leur abolition. Ainsi, en avril 2021, l'Union américaine pour les libertés civiles (ACLU) et la *Civil Rights Litigation Initiative* de la Faculté de droit de l'Université du Michigan ont intenté une action en justice au nom de Robert Williams, un an après que celui-ci ait été accusé et détenu préventivement à tort, sur foi d'une reconnaissance erronée par le dispositif de la police de Détroit (Ryan-Mosley, 2021). Ces initiatives ont poussé d'autres villes et Etats américains à légiférer en la matière (Spivack/Garvie, 2020). Enfin, une série d'auditions très éclairantes auprès du *House Oversight and Reform Committee* du Congrès américain[8] a donné lieu à des propositions de lois au niveau fédéral, qui pourraient encadrer plus drastiquement le recours à ces dispositifs (Learned-Miller *et al.*, 2020).

En Europe, la cartographie des différents usages et tentatives de régulations des TRF dans neuf pays, réalisée par Lequesne Roth *et al.* (2020), montre qu'aucun des Etats soumis à analyse ne s'est, à ce jour, doté d'une législation

8 Auditions accessibles sous : ‹https://www.c-span.org/video/?460959-1/house-hearing-facial-recognition-technology› (consulté le 21.4.21).

spécifique y relative. Leur diagnostic rend compte, en revanche, d'une multiplication d'expérimentations concernant ces dispositifs, y compris les LTRF, sans grand débat cependant, sinon à l'issue des quelques rares recommandations émises par les préposés à la protection des données. Aux termes du Règlement général sur la protection des données (RGPD, nº 2016/679) et de la Directive « Police-Justice » (nº 2016/680) de l'Union européenne, tout usage de ce type de technologies devrait *être soumis a minima à une* analyse d'impact. Leur financement et leur expérimentation doivent impérativement reposer sur des bases légales érigeant de robustes protections, s'agissant notamment de la prohibition de tout lien entre des bases de données gouvernementales et privées. Enfin, une exigence de transparence devrait diligenter le travail des entreprises impliquées en ce domaine, qui ne devraient en aucun cas pouvoir *évoquer le secret commercial pour se soustraire* à l'examen du public. Le projet de régulation de la Commission européenne présenté le 21 avril 2021 ajoute des cautelles supplémentaires aux LRTF, les élevant au rang de « système AI à haut risque » (European Commission, 2021). Aux termes de l'article 5 du projet, l'usage des LTRF par la police à des fins de maintien de l'ordre est, en principe, interdit, *à l'exception de trois situations*. Les LTRF pourront ainsi être *déployées notamment pour prévenir* « une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique de personnes physiques ou une attaque terroriste », *ou encore détecter, localiser et identifi*er l'auteur ou un suspect d'une infraction passible d'une sanction privative de liberté d'une durée de trois ans au moins. Ces situations requièrent une autorisation judiciaire, sauf si jugées urgentes par les autorités, qui pourront alors recueillir celle-ci *a posteriori*. De plus, les conditions *évoquées* ne s'appliquent pas aux acteurs de la sécurité privée. En somme, ces exceptions permettent une certaine appréciation des événements et offrent une certaine marge de manœuvre. Elles entérinent l'appel à un moratoire pourtant encore réitéré récemment par plus de 50 organisations activ(ist)es dans le domaine digital[9]. Pour nombre d'observateurs, cette option a été privilégiée pour laisser à des pays la possibilité de les intégrer, le cas échéant, dans leur arsenal sécuritaire[10]. Tel est le cas de la France, par exemple, où l'Assemblée nationale vient d'adopter dans la controverse une « loi relative à la sécurité globale », qui prévoit, entre autres, la surveillance par drones de rassemblements de personnes sur la voie publique (art. 22), engins susceptibles d'être conjugués un jour à un algorithme de reconnaissance faciale.

En Suisse, les discussions entourant les défis de tels dispositifs ont du mal à dépasser le cercle des initiés (Algorithm Watch, 2020). Il n'existe pas de base légale *sui generis* pour leur usage, mais notre arsenal législatif est si éclaté et la

9 Lettre ouverte accessible ici : ‹https://www.article19.org/wp-content/uploads/2021/04/Letter-from-51-civil-society-organisations-seeking-your-support-for-a-ban-on-biometric-mass-surveillance-practices.pdf› (consulté le 21.4.21).

10 Voir p. ex. les sites ‹https://presse-citron.net›, ‹https://zdnet.fr› et ‹https://laquadrature.net›.

nouvelle Loi sur la protection des données si peu « ambitieuse » (Métille, 2021), qu'il pourrait être possible d'esquiver avec la loi en lançant, par exemple, des projets-pilotes. En effet, l'infrastructure susceptible d'être couplée à ce type de technologie est déjà en place, puisqu'on évalue à environ 30 000 le nombre de caméras de vidéosurveillance déployées dans les espaces publics helvétiques. Au vu des expériences actuelles sur le continent, il n'est pas totalement inenvisageable que ces caméras se voient combinées à un algorithme de reconnaissance faciale à titre d'essai, ou qu'un tel algorithme soit conjugué aux *body-cams* actuellement en test dans plusieurs corps de police.

3.3 Enjeux de gouvernance

Les services de l'Etat, et particulièrement ceux de la police, ont accès à des outils de reconnaissance faciale depuis plusieurs décennies, mais ils se sont jusqu'alors généralement limités à ceux développés par leurs propres moyens et sur foi de leur propre collection d'images, typiquement des photos d'identité judiciaire ou de permis de conduire. Ces dernières années, toutefois, les choses ont évolué très rapidement, à tel point que certaines entités étatiques s'appuient désormais sur des outils et bases de données qui ne relèvent plus toujours de leur contrôle (Ferguson, 2021).

Cette situation s'explique en partie par une pratique « du pied dans la porte » de la part de certaines entreprises prédatrices de données. Les collaborations d'Amazon avec des centaines de corps de police aux Etats-Unis en sont une illustration. Dans un premier temps, ces derniers ont laissé Amazon développer son outil d'apprentissage machine, l'*Amazon Rekognition*, sur leurs bases de données existantes. Dans un deuxième temps, Amazon a entrepris de recueillir aussi ses propres images, typiquement via *RING,* son système de sonnette « intelligente » fondée sur la reconnaissance des images. Dans ce cadre, l'entreprise a noué des partenariats avec plus de 1000 polices locales et communautés[11], sous l'égide d'un *Digital Neighborhood Watch program* auquel est affilié sa *Neighbors App*, exploité également par ses partenaires policiers (Benton, 2019). Tout aussi récemment, la Gendarmerie royale du Canada et plusieurs services de police municipaux canadiens ont mis fin à leurs relations avec l'entreprise Clearview AI (Castets-Renard *et al.*, 2020). Plus de 600 services de police aux Etats-Unis se sont aussi dotés de l'application de reconnaissance faciale de cette entreprise, sérieusement critiquée pour avoir alimenté sa base de données de plus de 3 milliards d'images siphonnées sur des réseaux sociaux, des sites de vidéos en streaming, de paiements mobiles, ou

11 Voir la cartographie du réseau d'Amazon Ring sous : ‹https://www.google.com/maps/d/viewer?mid=1eYVDPh5itXq5acDT9b0BVeQwmESBa4cB&ll=36.19459170250789%2C-103.96982876449249&z=3› (consulté le 21.4.21).

encore de recrutement (Hill, 2020)[12]. Une situation dont l'Amérique du Nord n'a pas le monopole, puisqu'en avril 2021, la police criminelle finlandaise faisait son *mea culpa* pour y avoir également recouru[13].

En janvier 2020, l'agence Reuters dévoilait avoir consulté la version préliminaire du rapport de la Commission européenne sur la régulation de l'intelligence artificielle, annonçant l'imposition d'un moratoire sur les technologies de reconnaissance faciale à des fins d'identification à distance dans les espaces publics. Précurseur de la proposition de réglementation dont il a été question dans la section 3.2 ci-dessus, ce Livre blanc a été publié en mars 2020, peu de temps après le scandale *Clearview*. Il reconnaît expressément que les LTRF présentent de grands risques de porter atteinte aux droits fondamentaux, à la vie privée, à la diversité et au « vivre-ensemble » (Commission européenne, 2020, 25). Pour autant, le moratoire en question a été supprimé de la version officielle du Livre blanc, décision confirmée dans le projet de régulation d'avril 2021. Cet épisode démontre la difficulté des gouvernements à déjouer l'emprise des (lobbys) industriels, qui sapent le pouvoir des autorités légitimes de les réguler et de les surveiller. En filigrane, il révèle aussi la faible résistance opposée par les entités préposées à la sécurité à la détermination des industriels à poursuivre leur commerce très lucratif.

3.4 Enjeux de surveillance

La position dominante des acteurs du marché des données et dispositifs y affiliés fragmente le monopole de la puissance publique dans le champ du maintien de l'ordre et de la sécurité, ce qui pose des défis délicats, notamment en termes de confiance, de responsabilité, de transparence, d'équité, d'égalité et de justice sociale (O'Neil, 2016). Plus subrepticement, ces dispositifs ouvrent la voie à une « suspectification » de masse, pouvant aller jusqu'à un renversement des principes généraux qui font d'un Etat de droit, un Etat de droit, à commencer par celui de la présomption d'innocence. En colligeant indistinctement les images de visages dans les espaces publics, les LTRF traduisent, en effet, « *un* changement de paradigme de la surveillance (…) : le passage d'une surveillance ciblée de certains individus à la possibilité d'une surveillance de tous aux fins d'en identifier certains » (CNIL, 2019, 7).

Nombre de travaux portant sur le caractère intrusif de ces dispositifs se concentrent sur des aspects relevant de la vie privée et, plus récemment, leur

12 A noter que cette affaire a eu des retentissements en Suisse également. Dans le cadre de l'enquête menée à son propos par le Préposé fédéral à la protection des données, fedpol et le Service de renseignement de la Confédération, notamment, ont confirmé qu'ils « n'utilisaient ni n'avaient l'intention d'utiliser » dans leurs activités de dispositif du type de celui de Clearview. V. communiqué de presse du 10.3.2020 du PFPD.

13 Voir communiqué de presse du 9.4.2021 du Centralkriminalpolisen (CKP).

« *chilling effect* » sur l'exercice des libertés d'expression, de réunion et d'association (London Policing Ethics Panel, 2019). Ce qui demeure encore peu investi, en revanche, c'est la façon dont ces technologies s'inscrivent dans une dynamique de surveillance poreuse alimentée par une multiplication de « *little brothers* » ; en d'autres termes un « *crowdsourced surveillance network* » (Lally, 2017). Bauman parle de surveillance « liquide » pour encapsuler l'évolution silencieuse mais vertigineuse des configurations socio-techniques vouées au suivi, au traçage, au tri, au contrôle et à l'observation systématique d'un nombre toujours plus grand de facettes de nos existences (Bauman/Lyon, 2013). Cette grille de lecture rend compte également de la prolifération des acteurs qui y participent et, en particulier, de la façon dont nous sommes tous surveillés et surveillants à la fois. Le développement des LTRF n'est plus l'apanage de l'ingénierie des entreprises privées et des recherches universitaires. Il suffit de prendre un « *crash course* » pour développer son propre algorithme de reconnaissance faciale à l'aide d'un code *open source* disponible gratuitement, par exemple sur OpenCv. C'est d'ailleurs ainsi que naquit *Facewatch*, de l'initiative d'un individu, Simon Gordon, tenancier d'un bar déterminé à endiguer définitivement les vols et les comportements inadéquats dans son établissement. A l'appui d'un travail d'investigation détaillé, Devlin (2019) montre comment Gordon, grâce à un système de caméra placé à l'entrée de son établissement, conjugué à un logiciel standard d'analyse de reconnaissance faciale, a élaboré progressivement une liste de personnes d'intérêt, désormais alimentée par les abonnés auxquels *Facewatch* fournit ses services. Sur son site internet, son entreprise se targue d'être le détenteur de « la seule liste nationale de surveillance partagée pour la reconnaissance faciale en Grande-Bretagne » et « d'arrêter le crime avant même qu'il ne se produise »[14]. Elle envisage, d'ici à 2022, le déploiement de 5000 nouvelles caméras aux abords de lieux privés jouxtant des espaces publics, typiquement des bars, clubs, stations-service, hôtels et stades de sport, régulées par son algorithme de reconnaissance faciale et reliées à sa « *watch list* », élaborée « *homemade* ».

Les LTRF participent de la normalisation de l'(auto-)surveillance, bien au-delà du « *big brother orwellien* ». Comme le soulignent Bauman et Lyon (2013, 11), désormais la surveillance « *works at a distance in both space and time, circulating fluidly with, but beyond, nation-states in a globalized realm. Reassurance and rewards accompany those mobile groups for whom such techniques are made to appear ‹ natural ›. Profiling processes and exclusionary measures await the groups unlucky enough to be labelled ‹ unwelcome ›* ». Dès lors qu'elles les impactent directement, la participation des citoyen.ne.s à la discussion les concernant apparaît cruciale d'un point de vue démocratique. Leur implication requiert toutefois un certain niveau de connaissance de ces dispositifs, qui leur fait souvent défaut.

14 Voir ‹https://www.facewatch.co.uk/› (consulté le 21.4.21).

3.5 Enjeux de connaissance

Tel qu'en atteste la dernière étude en date menée auprès de plus de 4000 personnes au Royaume-Uni sur leur attitude face à la reconnaissance faciale, le public ne sait pas clairement comment la technologie est développée, acquise, comment elle fonctionne et dans quels buts (Ada Lovelace Institute, 2019). Alors que ces dispositifs sont en pleine extension dans ce pays, à la question de savoir « Dans quelle mesure êtes-vous conscient(e) de l'utilisation des systèmes de reconnaissance faciale ? », près de 90 % des sondés disent en être certes conscients, mais seulement 5 % rapportent savoir ce dont il s'agit et près de 85 % avouent n'y connaître rien ou très peu sur le sujet. Or, l'incompréhension du public sur ces dispositifs peut avoir pour conséquence tantôt de leur prêter à tort des capacités à juguler tous les problèmes de criminalité (Bromberg *et al.*, 2020), tantôt de miner sa confiance en les entités chargées du maintien de l'ordre, voire de se retourner contre leurs intervenants (Bradford *et al.*, 2020).

Au-delà, il paraît important que les citoyens puissent disposer de connaissances suffisantes sur ces dispositifs pour engager un débat contradictoire sur leurs avantages et leurs risques, et convenir de ce qui leur paraît ou non acceptable. A l'ère de la toute-puissance du « *self(ie)* », les périls entourant les technologies qui recourent à nos visages sont immenses en termes de classification, de discrimination, de surveillance de masse et de mauvaise gouvernance. Pour autant, les entreprises dominantes dans le recueil massif de données personnelles et des centaines d'autres profilées dans le champ de celles des visages[15] perfectionnent leurs dispositifs à leur aise, en se nourrissant allégrement des images que nous-mêmes leur fournissons. Combien d'algorithmes ont-ils été formés sur les images de nos enfants, placardées sur des profils *Whatsapp*, introduites dans des applications pour les retoucher, ou encore théâtralisées dans nos interactions sur les réseaux sociaux ? Par une socio-histoire des données de reconnaissance faciale, Raji et Fried (2021) dégagent quatre grandes ères de la recherche académique et commerciale dévolue à perfectionner les dispositifs qui s'en gorgent. Leurs « innovations » ont mené à étendre le champ d'application matériel des « galleries » – par exemple, par l'ajout de métadonnées portant notamment sur l'âge ou l'origine éthique des sujets –, mais aussi territorial, irriguées non plus seulement d'images tirées de bases de données officielles, mais aussi, par exemple, de recherches aléatoires sur l'internet, au mépris du consentement des sujets.

15 Telles que Facewatch, Face-Six, Kairos, Face++, FaceFirst, TrueFace, Faception, ou encore Anyvision, dont le logiciel de LTRF a été testé lors du carnaval de Nice en 2019. A son issue, le maire et les parties prenantes ont conclu que le dispositif participait à la « sécurisation des espaces publics », (Ville de Nice, 2019, 23). En dépit d'une évaluation rigoureuse, mais en écho au moto de l'entreprise, qui se targue également de « *making the world safer through visual intelligence* ».

Dans le domaine du maintien de l'ordre et de la sécurité, certaines entreprises ont, certes, réfréné leur ardeur quant au développement de leurs logiciels dédiés, notamment sous la pression des mobilisations suivant le meurtre de George Floyd par le policier Derek Chauvin à Minneapolis en mai 2020[16]. En été 2020, IBM a annoncé qu'elle cessait ses recherches dans ce domaine, Microsoft a communiqué qu'elle retirait ses logiciels de la vente aux forces de police américaines et Amazon, qu'elle les suspendait temporairement. Leur intention semble toutefois provisoire. Pour preuve, Microsoft et Amazon viennent de s'associer pour se défendre contre deux procès jumelés intentés à Seattle, qui remettent en cause la façon dont elles ont construit leurs algorithmes de reconnaissance (Long, 2021). Dans l'intervalle, les utilisateurs de Facebook typiquement, continuent d'y télécharger chaque jour des centaines de millions de photos, à tel point que l'entreprise détiendrait, selon ses termes, « le plus grand ensemble de données faciales au monde » (Taigman *et al.* 2014). S'ils ne se sont pas expressément désinscrits, *DeepFace*, son système de reconnaissance faciale à apprentissage profond, s'améliore sur leurs images ainsi partagées. Dans ces conditions, il semble pertinent d'entreprendre une démarche plus offensive d'éducation et d'information pour permettre à tout un chacun de prendre une position plus éclairée sur sa participation, même indirecte, à cet assemblage. En parallèle aussi, il conviendrait de renforcer la protection contre toutes représailles des développeurs de ces technologies lançant l'alerte sur leurs détournements (Crawford, 2019).

4. Vers un débat plus démocratique sur l'opportunité du recours à de tels dispositifs ?

Nos visages ont beau être uniques, ils sont toujours plus exposés, capturés et exploités. Dans la droite ligne de ce que certains nomment la « *first wave of algorithmic accountability* », les premières remises en question des dispositifs de reconnaissance faciale ont surtout tourné autour d'enjeux de « *fairness* ». Les travaux se sont ainsi multipliés pour résoudre leurs failles « techniques », en particulier centrées sur les biais (FAT/ML, 2018 ; Whittaker *et al.*, 2018 ; Latonero, 2018 ; Learned-Miller *et al.*, 2020). Or, ces démarches éludent une approche plus structurelle et systémique de la pénétration de ces technologies dans nos activités et interactions humaines. Irrigués des expériences et témoignages recueillis par des associations sur le terrain qui documentent leurs coûts humains et sociaux, les tenants de la « *second wave of algorithmic accountability* » nous invitent plutôt à nous interroger sur les causes structurelles entourant l'engouement qui leur est porté et l'opportunité même de leur

16 Derek Chauvin a été condamné en avril 2021. A l'heure où nous écrivons, il est probable que le condamné fera appel de ce jugement.

existence (Powles, 2018 ; Pasquale/Cockfield, 2018). Ensemble, ces travaux suscitent des questions d'intérêt public sur l'écosystème des données et les dispositifs y affiliés (Tableau 1).

Questions
Quels sont les problèmes auxquels la technologie prétend répondre ? Qui les définit ? Avec quels seuils d'acceptation et de confiance ?
Qui est à l'origine de la technologie et quelles sont au juste ses finalités ? Quels idéaux (voire idéologies) traduit-elle ?
Avec quels financements et bénéfices attendus ?
Où et comment la technologie a-t-elle été développée ?
Est-ce possible de garantir la provenance et l'exactitude des données saisies et exploitées ? Où, comment et sur quelle durée sont-elles stockées, archivées et qui en a l'accès ?
Son code est-il accessible pour garantir la transparence et les responsabilités ?
Sous quel(s) contrôle(s) la technologie a-t-elle été développée et le demeurera-t-elle si elle venait à être déployée ?
La technologie a-t-elle été testée, avec quels résultats ?
Qui sera en charge de sa maintenance ? A quels coûts ?
Quelles seront les formations offertes et le suivi réalisé auprès des praticiens dédiés à son utilisation ?
Comment les pratiques à l'appui de la technologie affecteront-elles les relations des institutions avec celles et ceux qui les concernent et la communauté dans son ensemble ?
Sera-t-elle utilisée d'une manière qui respecte l'autonomie et la dignité des personnes qu'elle affectera ?

Tableau 1 : Exemples de questions pour un écosystème vigilant

Ces questions invitent les décideurs, les institutions, les intervenants professionnels et les citoyens à un « réflexe réflexif » avant d'émettre une opinion sur, d'acquérir et d'utiliser le cas échéant ces dispositifs. En amont, elles devraient guider leurs développeurs à tous les stades de leur élaboration. Plus largement, elles convient tout un chacun à s'engager dans un dialogue sérieux sur les choix que ces dispositifs impliquent forcément et à les réévaluer ponctuellement, dès lors qu'ils façonnent la fabrique du social et les trajectoires individuelles (Binns, 2018).

5. Discussion : Qui pour définir « un monde plus sûr » ?

Il existe aujourd'hui un marché colossal, mais largement non réglementé, de technologies vendues au motif d'améliorer les performances des entités préposées à la sécurité des biens, des personnes et des infrastructures, parmi lesquelles figurent les (L)TRF. Dans un contexte sociétal qui tolère difficilement

la réalisation des risques, y compris des risques criminels, il n'est pas étonnant que ces entités voient en ces technologies une opportunité de parfaire leurs activités en termes de détection, de prévention, d'investigation et toujours plus d'anticipation. Les (L)TRF ne sont qu'un exemple parmi d'autres de la rencontre des « *big data analytics* », des appareillages biométriques et de l'intelligence artificielle qui, conjuguées, participent à ventiler les individus dans des catégories présumées plus ou moins à risque de poser des « problèmes ». Ces « problèmes » peuvent être de nature criminelle, mais peuvent tout aussi bien être affiliés à l'accès au logement, à la santé, à la scolarité ou encore à l'emploi. Ils concernent tout un chacun·e désormais sujet·te à un *screening* quotidien, et disqualifient plus aisément certains groupes de populations, plus vulnérables aux incertitudes socio-économiques et au contrôle social dans toutes les facettes de leur existence (Eubanks, 2018).

En définitive, les (L)TRF en appellent certes à la plus grande vigilance. Là où elles sont déployées, même à titre d'« expérimentation », elles cumulent de périlleuses audaces : elles portent atteinte au respect des droits de l'homme et des libertés et pêchent par absence de base légale, par opacité et par dilution des responsabilités. Ce sont toutefois moins les technologies elles-mêmes qui interrogent, que ce qu'elles traduisent de notre rapport au monde. D'abord, l'importance accrue que prennent les images dans tous les domaines de la vie en société, comme les difficultés que nous avons de nous affranchir des infrastructures qui les recueillent, tels que les CCTV, réseaux sociaux et téléphones portables (Keyes, 2019). Ensuite, la préséance de la rationalité néolibérale qui les imprègne et, à travers elles, reproduit son système de privilèges et perpétue les inégalités (Smith, 2020). Enfin, la reconfiguration progressive des savoirs et des pouvoirs entre les protagonistes – publics et privés, humains et non-humains – impliqués dans le contrôle social (Andrejevic et Selwyn, 2020). En prenant nos visages en objet de gouvernance, ces dispositifs participent à un post-panoptique diligenté à distance en grande partie par des acteurs privés, dont la définition de la « justice » et la poursuite d'un « monde plus sûr » se devraient d'être plus largement disputées.

Références

Ada Lovelace Institute, Beyond Face Value: Public Attitudes to Facial Recognition Technology, London, 2019.

Algorithm Watch, Automating Society Report 2020, Berlin 2020.

Andrejevic M./Selwyn N., Facial Recognition Technology in Schools: Critical Questions and Concerns, Learning, Media and Technology 2/2020, 115 ss.

Agüera y Arcas B./Mitchell M./Todorov A., Physiognomy's New Clothes, in: Medium May 7, 2017.

Bauman Z./Lyon D., Liquid Surveillance : A Conversation, Cambridge 2013.

Benton J., The Doorbell Company That's Selling Fear, in: The Atlantic May 1, 2019.

Binns R., Algorithmic Accountability and Public Reason, Philosophy and Technology 4/2018, 543 ss.

Biometrics and Forensics Ethics Group, Briefing Note on the Ethical Issues Arising from Public-private Collaboration in the Use of Live Facial Recognition Technology, January 2021.

Blount K., Body Worn Cameras with Facial Recognition Technology: When it Constitutes Search, Criminal Law Practitioner 3(4)/2017, 61 ss.

Bradford B./Yesberg J. A./Jackson J./Dawson P., Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support For Police Use of New Technology, The British Journal of Criminology 6/2020, 1502 ss.

Bromberg D. E./Charbonneau E./Smith A., Public Support for Facial Recognition Via Police Body-Worn Cameras: Findings From a List Experiment, Government Information Quarterly 1/2020, 1014 s.

Buolamwini J./Gebru T., Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Conference on Fairness, Accountability, and Transparency (FAT), Proceedings of Machine Learning Research 81/2018, 1 ss.

Buolamwini J./Ordóñez V./Morgenstern J./Learned-Miller E., Facial Recognition Technologies : A Primer, 2020.

Cardon D., A quoi rêvent les algorithmes ? Nos vies à l'heure des big data, Paris 2015.

Castets-Renard/Guiraud E./Avril-Gagnon J., Cadre juridique applicable à l'utilisation de la reconnaissance faciale par les forces de police dans l'espace public au Québec et au Canada, Ottawa 2020.

CNIL, Reconnaissance Faciale : pour un débat à la hauteur des enjeux, 15 novembre 2019.

Commission européenne, Livre blanc, Intelligence artificielle : Une approche européenne axée sur l'excellence et la confiance, COM 65/2020 final.

Crawford K., Regulate Facial-Recognition Technology, Nature 572/2019, 565.

Crawford K., The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence, New Haven 2021.

Devlin H., 'We Are Hurtling Towards a Surveillance State': the Rise of Facial Recognition Technology, in: The Guardian, October 5, 2019.

Eubanks V., Automating Inequality : How High-Tech Tools Profile, Police, and Punish the Poor, New York 2018.

European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artifical Intelligence

(Artificial Intelligence Act) and Amending Certain Union Legislative Acts, 2021.

FAT/ML, Principles for Accountable Algorithms and a Social Impact Statement for Algorithms, ‹https://www.fatml.org/resources/principles-for-accountable-algorithms›.

Ferguson A. G., Facial Recognition and the Fourth Amendment, Minnesota Law Review 3/2021, 1105 ss.

Foucault M., Surveiller et punir. Naissance de la prison, Paris 1975.

Fussey P./Murray D., Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology (The Human Rights, Big Data and Technology Project), UK 2019.

Fussey P./Davies B./Innes M., 'Assisted' Facial Recognition and the Reinvention of Suspicion and Discretion in Digital Policing, The British Journal of Criminology 2/2021, 325 ss.

Garvie C./Bedoya A./Frankle J., The Perpetual Line-Up: Unregulated Police Face Recognition in America, Washington 2016.

Garvie C., Garbage In, Garbage Out: Face Recognition on Flawed Data, Washington 2019.

Gates K. A., Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance, New York 2011.

Grother P./Ngan M./Hanaoka, K., Face Recognition Vendor Test (FRVT) Part 2: Identification & Part 3 : Demographic Effects, 2019, ‹https://doi.org/10.6028/NIST.IR.8271 & https://doi.org/10.6028/NIST.IR.8280›.

Hannah-Moffat K., Algorithmic Risk Governance: Big Data Analytics, Race and Information Activism in : Criminal Justice Debates, Theoretical Criminology 4/2019, 453 ss.

Hill K., The Secretive Company That Might End Privacy as We Know It, in: The New York Times, January 20, 2020.

Hooker S., Moving Beyond "Algorithmic Bias is a Data Problem", in: Patterns 2, April 9 2021, 1 ss.

Introna L. D./Wood D., Picturing Algorithmic Surveillance : The Politics of Facial Recognition Systems, Surveillance & Society 2-3/2004, 177 ss.

Jacquet M./Grossrieder L., Enjeux et perspectives de la reconnaissance faciale en sciences criminelles, Criminologie, 1/2021, 135 ss.

Joseph G./Lipp K., IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search by Skin Color, in: The Intercept, September 6, 2018.

Keyes O., The Bones We Leave Behind, in: Real Life, October 9, 2019.

Lally N., Crowdsourced Surveillance and Networked Data, Security Dialogue, 1/2017, 63 ss.

Latonero M., Governing Artificial Intelligence: Upholding Human Rights & Dignity, New York 2018.

Learned-Miller E./Ordóñez V./Morgenstern J./Buolamwini, J., Facial Recognition Technologies in the Wild: A Call for a Federal Office, 2020.

Lequesne Roth C. (sous la dir.), La reconnaissance faciale dans l'espace public : Une cartographie juridique européenne, 2020.

London Policing Ethics Panel, Interim Report on Live Facial Recognition, July 2018.

London Policing Ethics Panel, Final Report on Live Facial Recognition, May 2019.

Long K. A., Amazon and Microsoft Team Up to Defend Against Facial Recognition Lawsuits, in: The Seattle Times, April 15, 2021.

Métille S., Le traitement de données personnelles sous l'angle de la (nouvelle) Loi fédérale sur la protection des données du 25 septembre 2020, Semaine Judiciaire 2021 (II), 1 ss.

Metropolitan Police, Response to the London Policing Ethics Panel Final Report on Live Facial Recognition Technology, January 23, 2020.

Mohamed S./Png M.-T./Isaac W., Decolonial AI: Decolonial Theory as Sociotechnical Foresight in Artificial Intelligence, Philosophy & Technology 4/2020, 659 ss.

O'Neil C., Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, New York 2016.

Pasquale F./Cockfield A. J., Beyond Instrumentalism: A Substantivist Perspective on Law, Technology, and the Digital Persona, Michigan State Law Review 4/2018, 821 ss.

Powles J., The Seductive Diversion of 'Solving' Bias in Artificial Intelligence, in: OneZero, December 7, 2018.

Raji I. D./Fried G., About Face: A Survey of Facial Recognition Evaluation, in: Association for the Advancement of Artificial Intelligence, arXiv:2102.00813 [cs.CV], February 2021.

Raviv S., The Secret History of Facial Recognition, in: Wired, January 21, 2020.

Ryan-Mosley T., The New Lawsuit that Shows Facial Recognition is Officially a Civil Rights Issue, in: MIT Technology Review, April 14, 2021.

Smith G., The Politics of Algorithmic Governance in the Black Box City, in: Big Data & Society, July-December 2020, 1 ss.

Spivack J./Garvie C., A Taxonomy of Legislative Approaches to Face Recognition in the United States, in: Kak A. (éd.) Regulation Biometrics: Global Approaches and Urgent Questions, Washington 2020, 86 ss.

Taigman Y./Yang M./Ranzato M./Wolf L., DeepFace: Closing the Gap to Human-Level Performance in Face Verification, in: IEEE Conference on Computer Vision and Pattern Recognition, 2014, 1701 ss.

The Law Society of England and Wales, Algorithms in the Criminal Justice System, London 2019.

Ville de Nice, Rapport – Expérimentation reconnaissance faciale, in : Police Municipale et Maire de Nice, 20 juin 2019.

Whittaker M./Crawford K./Dobbe R./Fried G./Kaziunas E./Mathur V./Myers West S./Richardson R./Schultz J./Schwartz O., AI Now Report 2018, New York 2018.

Wiles P., Commissioner for the Retention and Use of Biometric Material : Annual Report 2018, London 2019.

Wiles P., Commissioner for the Retention and Use of Biometric Material : Annual Report 2019, London 2020.

Yan W., Face-Mask Recognition Has Arrived – For Better or Worse, in: The National Geographic, September 11, 2020.