Criminologie

Enjeux et perspectives de la reconnaissance faciale en sciences criminelles
Challenges and perspectives to face recognition in criminal science
Desafíos y perspectivas del reconocimiento facial en las ciencias penales

Maëlig Jacquet et Lionel Grossrieder

Volume 54, numéro 1, printemps 2021

Image et justice

URI : https://id.erudit.org/iderudit/1076696ar
DOI : https://doi.org/10.7202/1076696ar

Aller au sommaire du numéro

Éditeur(s)

Les Presses de l'Université de Montréal

ISSN

0316-0041 (imprimé)
1492-1367 (numérique)

Découvrir la revue

Citer cet article

Jacquet, M. & Grossrieder, L. (2021). Enjeux et perspectives de la reconnaissance faciale en sciences criminelles. *Criminologie*, *54*(1), 135–170. https://doi.org/10.7202/1076696ar

Résumé de l'article

L'objectif de cet article est de cristalliser de manière pragmatique les enjeux et perspectives de la reconnaissance faciale en sciences criminelles pour acquérir une meilleure connaissance des limitations et des opportunités offertes par ces technologies, essentielles à leur application au sein du système judiciaire. Nous postulons que cette réflexion doit s'inscrire dans une approche interdisciplinaire qui intègre l'utilisation d'algorithmes en considérant les spécificités de la criminologie et de la science forensique. Cet éclairage permet d'établir un bilan de l'utilisation de la reconnaissance faciale en le scindant en questions fondamentales. Quelles sont les images utilisées en reconnaissance faciale ? Comment sont-elles comparées ? Quels objectifs la reconnaissance faciale sert-elle ? Où est-elle mise en oeuvre et par quels acteurs ? Cette subdivision permet de mieux situer les enjeux et limites de la reconnaissance faciale, ainsi que les perspectives de développement et de recherche. Sur le plan des données elles-mêmes, l'enjeu principal concerne leur qualité originale puis sa dégradation potentielle aux stades de collecte et de sauvegarde des images, qui influencent leur utilisation ultérieure. Pour ce qui est des méthodes, les enjeux se cristallisent autour du manque de standardisation et de transparence, aussi bien lors de tâches exécutées par l'être humain que par un système automatique. Concernant les objectifs des tâches de reconnaissance faciale dans les domaines civil et judiciaire, les enjeux gravitent autour de la protection de la sphère privée et des libertés individuelles. Enfin, les principaux défis soulevés par son utilisation comme moyen de preuve au tribunal concernent la communication, ainsi que la standardisation et la validation méthodologique.

Enjeux et perspectives de la reconnaissance faciale en sciences criminelles

Maëlig Jacquet[1]
Étudiante au doctorat
École des sciences criminelles, Université de Lausanne, Suisse
maelig.jacquet@unil.ch

Lionel Grossrieder
Responsable de recherche
École des sciences criminelles, Université de Lausanne, Suisse
lionel.grossrieder@unil.ch

RÉSUMÉ • *L'objectif de cet article est de cristalliser de manière pragmatique les enjeux et perspectives de la reconnaissance faciale en sciences criminelles pour acquérir une meilleure connaissance des limitations et des opportunités offertes par ces technologies, essentielles à leur application au sein du système judiciaire. Nous postulons que cette réflexion doit s'inscrire dans une approche interdisciplinaire qui intègre l'utilisation d'algorithmes en considérant les spécificités de la criminologie et de la science forensique. Cet éclairage permet d'établir un bilan de l'utilisation de la reconnaissance faciale en le scindant en questions fondamentales. Quelles sont les images utilisées en reconnaissance faciale ? Comment sont-elles comparées ? Quels objectifs la reconnaissance faciale sert-elle ? Où est-elle mise en œuvre et par quels acteurs ? Cette subdivision permet de mieux situer les enjeux et limites de la reconnaissance faciale, ainsi que les perspectives de développement et de recherche. Sur le plan des données elles-mêmes, l'enjeu principal concerne leur qualité originale puis sa dégradation potentielle aux stades de collecte et de sauvegarde des images, qui influencent leur utilisation ultérieure. Pour ce qui est des méthodes, les enjeux se cristallisent autour du manque de standardisation et de transparence, aussi bien lors de tâches exécutées par l'être humain que par un système automatique. Concernant les objectifs des tâches de reconnaissance faciale dans les domaines civil et judiciaire, les enjeux gravitent autour de la protection de la sphère privée et des libertés individuelles. Enfin, les principaux défis soulevés par son utilisation comme moyen de preuve au tribunal concernent la communication, ainsi que la standardisation et la validation méthodologique.*

1. École des sciences criminelles, Université de Lausanne, Batochime – 1015, Lausanne, Suisse.

MOTS CLÉS • *Reconnaissance faciale, image, action de sécurité, science forensique, élément de preuve.*

Introduction

À la fin du XIX^e^ siècle, le criminologue Alphonse Bertillon élabore des fiches signalétiques introduisant le visage, entre autres, comme moyen d'identification des criminels récidivistes (Bertillon, 1886). Aujourd'hui, la comparaison de visages et l'enregistrement d'images faciales sont omniprésents dans de nombreux domaines civils et judiciaires. La comparaison d'images faciales, appelée plus généralement reconnaissance faciale, permet d'apprécier le taux de ressemblance entre deux visages afin d'évaluer la possibilité qu'il s'agisse de la même personne ou de deux personnes distinctes. Ces opérations sont effectuées aussi bien manuellement, par exemple par un.e officier.ière des douanes qui compare l'image d'un document d'identité au visage de la personne présente, ou de manière automatisée, par exemple lors de la recherche dans de larges bases de données d'un individu inconnu visible sur des images de vidéosurveillance.

Les récentes innovations technologiques ainsi que la démocratisation des dispositifs d'enregistrement génèrent une quantité croissante d'images d'actes délinquants ou déviants. Dans un contexte forensique où l'image est une trace de ces activités, la reconnaissance faciale prend de plus en plus de place au sein du continuum pénal. Pour soutenir la prise de décision en matière d'action de sécurité, celle-ci s'apparente à un outil aux multiples fonctions, telles que le soutien aux enquêtes, la production de renseignement et la présentation d'éléments de preuve devant les tribunaux.

La littérature scientifique entourant la reconnaissance faciale se focalise majoritairement sur les problématiques techniques d'une part, notamment en termes de performances et de développements algorithmiques, et sur les dangers éthiques et sociétaux d'autre part. En revanche, peu d'études s'interrogent sur les applications actuelles et potentielles de ces méthodes et sur leur intégration, aussi bien dans un contexte civil que judiciaire. Leur perception par le public est idéalisée – ou au contraire diabolisée – par la représentation faite de la reconnaissance faciale dans les médias, tant réels que fictifs. Il est nécessaire de déconstruire les mythes et attentes (réalistes ou non) érigés pour entrevoir le potentiel et les limitations de cette technologie.

Dans cet article, nous proposons un vaste bilan de son utilisation dans un contexte criminologique et forensique, en décrivant succinctement les méthodes et types d'images utilisés, les domaines d'application, les objectifs et les acteurs qui interviennent. Ce constat nous permet ensuite d'ouvrir la discussion sur les atouts et problématiques et les besoins qu'ils soulèvent. Une importance particulière est accordée au regard transversal porté sur ce domaine, qui convoque des connaissances à la fois forensiques, liées à la méthodologie et aux objectifs poursuivis, criminologiques, liées aux différentes applications et réactions sociales, et numériques, liées aux algorithmes utilisés.

« Mythes » et attentes sociétales

Avec sa démocratisation grandissante, la reconnaissance faciale est accompagnée d'idées reçues véhiculées entre autres par les médias, fictionnels et réels, et les campagnes commerciales de systèmes de reconnaissance automatisée.

Depuis plus de dix ans, la reconnaissance faciale est présentée au grand public comme un outil « miracle » capable de fournir un résultat binaire irréfutable – « identification » ou « exclusion » – pour la reconnaissance de personne d'intérêt dans le cadre judiciaire. Dès les prémices du développement de cette technique, les séries télévisées, telles que *Les Experts*, *NCIS* et *Bones*, ont montré l'exploitation d'outils aux performances inespérées. À titre d'exemple, la Figure 1 est un extrait d'un épisode des *Experts*, datant de 2008, où un système automatique compare la photographie récente d'une personne âgée à une image d'archive représentant un jeune homme d'identité connue. L'algorithme de l'inspectrice forensique conclut en quelques instants et sans l'ombre d'un doute qu'il s'agit de la même personne. En réalité, la comparaison de ces deux images serait compliquée par le grand nombre d'années séparant les deux clichés, et par les multiples variations en termes de luminosité, d'angle de prise de vue (altérant les dimensions et proportions), de résolution et d'expressions faciales. Cela impacte le degré de similarité des deux visages et augmente le risque de résultats incorrects, ce qui diminue les performances aussi bien des systèmes de reconnaissance faciale que de l'être humain (Peng, 2019 ; Phillips *et al.*, 2018).

FIGURE 1

Extrait du processus de reconnaissance faciale présenté dans *Les Experts* (Saison 9, épisode 8, 2008)

Bien que l'effet de ces séries sur l'opinion publique, communément appelé *CSI effect*, demeure mitigé (Cole et Dioso-Villa, 2007 ; Smith, Stinson et Patry, 2011), cet exemple présente un éventail assez représentatif de problématiques couramment ignorées dans la fiction, pourtant toujours activement étudiées dans la littérature spécialisée. Les médias « réels » tels que la presse écrite et télévisée ne relatent que peu (voire pas) de détails sur l'utilisation judiciaire de ces technologies. En cause, la confidentialité des informations entourant des cas récents évidemment, mais également la faible utilisation des techniques de reconnaissance faciale dans ce domaine. En contrepartie, il existe et se développe une abondance d'articles, de débats, d'interviews, traitant de l'omniprésence des caméras et systèmes de surveillance des populations et de leurs dangers. Cette technologie est présentée comme un outil de surveillance massive mettant en danger le respect de la vie privée, mais dont la fiabilité dans certaines conditions serait médiocre (Davies, Innes et Dawson, 2018 ; Fussey et Murray, 2019).

Cette impression de performances miracles de la reconnaissance faciale est exacerbée par la croyance selon laquelle le système agit à notre place et accomplit successivement une multitude de tâches variées pour remplir son objectif final, telles qu'identifier un suspect, lier des délits et prouver la culpabilité ou non d'un auteur. Ici encore, les stratégies commerciales ainsi que les représentations médiatiques édulcorées mettent en avant une simplicité et une autonomisation presque complète tout en occultant un élément indispensable du processus, l'être humain. Nombre de tâches essentielles dépendent encore

presque exclusivement du facteur humain, comme par exemple, trier les images pertinentes, prétraiter les données pour les adapter à l'analyse, réviser et interpréter les résultats de comparaison. L'efficacité d'une tâche de reconnaissance faciale dépend donc d'un ensemble de choix et d'actions sur différents plans et ne découle pas uniquement de l'utilisation d'un outil informatisé.

Cependant, l'autonomisation et les performances idéalisées génèrent le besoin d'un système à la pointe de la technologie et supposé onéreux. Il n'est pas rare de confondre la complexité d'un logiciel et son efficacité. De la même manière que le nombre de pixels d'un appareil photo numérique est un puissant argument commercial pour le grand public, la mise en avant de la puissance de calcul d'un outil de reconnaissance faciale peut rapidement être assimilée à la qualité de ses résultats. De plus, cela risque de mener à une optimisation intrinsèque du système, c.-à-d. que l'algorithme crée ce qu'il cherche à décrire (O'Neil, 2016). La plupart des études sur les algorithmes automatiques sont effectuées sur des bases de données développées pour la recherche. Les outils qui en découlent présentent ainsi des performances élevées lorsqu'ils sont appliqués à ces données, mais lors d'une application en conditions réelles avec les contraintes et spécificités que cela implique, leur utilité peut se révéler décevante.

Ces différents amalgames et mécompréhensions de la reconnaissance faciale et de son utilisation dans un contexte d'action de sécurité peuvent s'avérer dangereux dès lors qu'ils s'inscrivent dans les problématiques plus larges liées aux grands volumes de données (*big data*). Avec le changement de type et de quantité de données traitées, c'est toute la méthodologie mise en place qui est susceptible d'être reconsidérée. Pour les décideurs, le plus simple est d'acquérir des logiciels automatisés, souvent présentés comme une solution miracle, afin de faire montre d'une préoccupation de modernisation de la police (Dupont, 2016). Devant cette modernisation croissante, il est essentiel de comprendre les avantages et les limites de la reconnaissance faciale.

État des lieux

Afin d'entamer une réflexion sur l'utilisation de la reconnaissance faciale dans le contexte de l'action de sécurité, et à la vue de nos précédentes observations, nous postulons que cette réflexion doit s'inscrire dans une approche interdisciplinaire qui intègre l'utilisation d'algorithmes en

considérant les spécificités de la criminologie et de la science forensique. Il est reconnu dans plusieurs domaines que le besoin de résoudre des problèmes sociaux intrinsèquement complexes et l'influence grandissante des nouvelles technologiques sont des moteurs puissants de l'interdisciplinarité (Committee on Facilitating Interdisciplinary Research, 2004). Ainsi, combiner la criminologie avec la science forensique permet d'établir un bilan de l'utilisation de la reconnaissance faciale en le décomposant en questions fondamentales. Quelles sont les images utilisées en reconnaissance faciale ? Comment sont-elles comparées ? Quels objectifs la reconnaissance faciale sert-elle ? Où est-elle mise en œuvre et par quels acteurs ?

Images et méthodes de comparaison

La reconnaissance faciale est utilisée dans trois principales tâches, selon le matériel à la disposition et l'objectif visé : la vérification (c.-à-d. la comparaison de deux images entre elles, dite « 1-v-1 »), l'identification (c.-à-d. la comparaison d'une image à une base de données de N images, dite « 1-v-N ») (ISO/IEC 2382-37 : 2017(E), 2017), et la supervision (c.-à-d. le suivi de l'image d'une personne dans une séquence vidéo, dite « 1-v-0 » (Castelluccia et Le Métayer, 2019 ; Marzouki, 2001).

a. Images

Pour chacune de ces tâches, les deux catégories principales d'images comparées entre elles sont les traces et les références.

Les traces, c.-à-d. les vestiges physiques et numériques d'activités litigieuses (Ribaux, 2014), sont les images de source inconnue enregistrées au moment des faits puis collectées. Elles permettent notamment de visualiser une ou plusieurs personnes et lieux d'intérêt. Par exemple, lors d'une investigation liée à l'utilisation frauduleuse de carte bancaire à la suite d'un vol à la tire, les enregistrements de la caméra de surveillance au moment du vol ainsi que ceux du distributeur automatique de billets (DAB) sont remis à la police, à sa demande. De telles images fournissent de nombreux renseignements aux enquêteurs. Il est ainsi possible de retracer le parcours de personnes d'intérêt (PI) avant ou après les faits, de distinguer leur morphologie, leurs vêtements et leur visage, puis, si la qualité le permet, de comparer le visage de la PI à des images de référence, par exemple la photographie d'un suspect (vérification) ou une base de données pour rechercher de potentiels suspects (identification).

Les références sont donc des images de source connue et de bonne qualité. Il s'agit le plus souvent de documents d'identité, permis de conduire ou d'images signalétiques. Lorsque l'investigation s'oriente vers une ou plusieurs PI grâce aux images-traces et que l'instruction requiert le travail d'un expert afin de présenter ses conclusions au tribunal, il est nécessaire d'acquérir des images de référence pour les comparer aux traces.

À l'instar de domaines tels que l'exploitation de traces digitales, la comparaison entre images-traces et images de référence peut être effectuée tant manuellement qu'à l'aide de systèmes automatiques. Dans les sections suivantes, nous présentons brièvement ces approches en soulignant leurs avantages et limitations pratiques.

b. Méthodes manuelles

La comparaison manuelle est utilisée pour des tâches nécessitant d'analyser peu d'images simultanément, par exemple lors de contrôles d'identité (comparaison d'une personne avec un document d'identité) et lors d'investigations judiciaires (comparaison d'une image de vidéosurveillance avec la photographie signalétique d'un.e prévenu.e). La littérature spécialisée décrit quatre méthodes d'analyse pour la comparaison manuelle de visages par un.e expert.e : holistique, morphologique, photo-anthropométrique et la superposition des deux images comparées (Ali, Veldhuis et Spreeuwers, 2012).

L'analyse holistique est la description globale des caractéristiques du visage, sans aucune mesure. Cette méthode est notamment utilisée par un.e officier.ière lors de contrôles d'identités à la douane, par exemple. Cela permet une comparaison rapide mais également très dépendante de la qualité des images et du degré de difficulté de la comparaison (forte ressemblance de personnes différentes). Dans un contexte judiciaire, il est recommandé de n'utiliser cette méthode qu'en première instance, en la combinant avec les approches suivantes, en raison de ces performances faibles et variables.

L'analyse morphologique consiste à décrire les formes et proportions des éléments du visage (front, yeux, nez, bouche, sourcils, oreilles, joues, menton) de la manière la plus précise possible. Cela comprend également la description des marques faciales (c.-à-d. rides, cicatrices, taches de rousseur, grains de beauté, tatouages, etc.) ainsi que la couleur et la longueur des cheveux, l'implantation et la densité de la pilosité. Lors d'expertises forensiques, cette pratique est considérée comme la

plus performante, applicable aux images de qualité variable et dont le processus est à la portée des personnes non spécialisées. Elle souffre cependant d'un manque de transparence et de standardisation, ainsi que d'une trop grande dépendance à la capacité innée de l'expert à reconnaître les visages, et à la qualité de l'image (Noyes, Phillips et O'Toole, 2017 ; Peng, 2019 ; Phillips *et al.*, 2018). Le « talent » inné d'une personne à reconnaître des visages prévaut de plus en plus dans des études comme celle de Towler et de ses collègues (2019), où les auteurs mettent en évidence l'inefficacité des programmes d'entraînement aux tâches de reconnaissance faciale dédiées aux experts.

La troisième approche, l'analyse photo-anthropométrique, repose sur les mesures de distance entre certains points du visage tels que la base du menton, le centre de la bouche et des yeux, les commissures des lèvres, les bords des ailes du nez, etc. (Moreton et Morley, 2011).

Enfin, la technique de superposition des images a pour but de visualiser plus directement les similarités et les discordances morphologiques et anthropométriques des visages sur les deux images.

Concernant l'applicabilité de ces deux méthodes, les Facial Identification Scientific Working Group (FISWG) et European Network of Forensic Science Institutes (ENFSI) recommandent de ne pas utiliser seules les approches anthropométriques et de superposition d'images à des fins de comparaison, et de combiner plusieurs approches (ENFSI, 2018 ; FISWG, 2012). En cause : (i) la nécessité d'utiliser des images prises dans des conditions optimales, ce qui est rarement le cas ; (ii) le caractère très chronophage de ces processus ; (iii) l'entraînement avancé dont l'opérateur a besoin, si tant est qu'il soit efficace ; et (iv) le manque de fiabilité des résultats. Dans le cadre judiciaire, les experts basent leurs comparaisons sur les approches validées et recommandées par les organismes compétents. Ces derniers conduisent régulièrement des tests de performance afin d'évaluer les résultats des protocoles individuels et d'adapter ses recommandations méthodologiques.

c. Systèmes automatiques

Le nombre croissant de comparaisons d'images nécessaire dans certains domaines a naturellement mené à l'automatisation du processus. Ainsi, un investigateur peut comparer une image-trace à toutes les images-références d'une base de données de délinquants connus.

Afin de mieux appréhender les enjeux liés à ces systèmes, nous proposons tout d'abord une brève présentation de leur fonctionnement.

Les systèmes automatiques sont développés sur la base de deux grands modèles algorithmiques : les moteurs de règles (*rule-based)* et l'apprentissage (*machine learning*) (Buchanan, 2005). Les algorithmes *rule-based* extraient d'une image les informations ciblées par le développeur puis les comparent pour évaluer le degré de similarité entre les informations d'une image A et celles d'une image B. L'ensemble du processus est donc transparent pour le développeur de l'algorithme et peut également l'être pour l'utilisateur si tant est que la totalité du code soit mise à la disposition du public (algorithmes *open source*). Jusqu'à récemment, la totalité des algorithmes était basée sur ce fonctionnement. Ces dernières années ont vu l'émergence et le prompt développement d'algorithmes basés sur un processus de *machine learning*, et plus spécifiquement de *deep learning* (apprentissage profond) (LeCun, Bengio et Hinton, 2015). Le système basé sur l'apprentissage est entraîné à détecter et reconnaître des visages à partir de larges bases de données, fournies par le/la développeur.euse (ou par l'opérateur.trice si l'algorithme est *open source*). Durant cette phase, le système collecte une multitude d'informations et génère ses propres règles lui permettant de détecter, analyser et comparer deux visages pour en évaluer la similarité. Les performances de ces systèmes sont donc étroitement liées aux données utilisées pour l'apprentissage. Par exemple, un système entraîné uniquement sur des photographies d'identité – frontales et de bonne qualité – sera peu performant sur des images de caméra de surveillance de mauvaise qualité et avec un angle de prise de vue variable (Peng, 2019).

Lors de leur utilisation par des institutions publiques ou privées, voire lors d'une investigation judiciaire, ces systèmes représentent une aide et un gain de temps précieux, et les potentielles erreurs peuvent être contrôlées *a posteriori* par un.e opérateur.trice ou investigateur.trice. Néanmoins, dans le cadre pénal, de telles erreurs sont proscrites en raison de leur trop important impact éventuel (incarcération ou libération à tort d'un.e prévenu.e). C'est pourquoi les systèmes automatiques de reconnaissance faciale sont encore peu exploités et que de nombreuses recherches tendent actuellement à développer des méthodes permettant l'utilisation de leurs résultats comme élément de preuve au tribunal (Ali *et al.*, 2012 ; Jacquet et Champod, 2020 ; Rodriguez, Geradts et Worring, 2018).

Les performances des systèmes de reconnaissance faciale les plus couramment utilisés ou récemment développés sont évaluées par le National Institute of Science Technology (NIST) dans ses rapports *Face*

Recognition Vendor Test (FRVT) (p. ex. : Grother, Ngan et Hanaoka, 2019).

Objectifs et domaines d'application

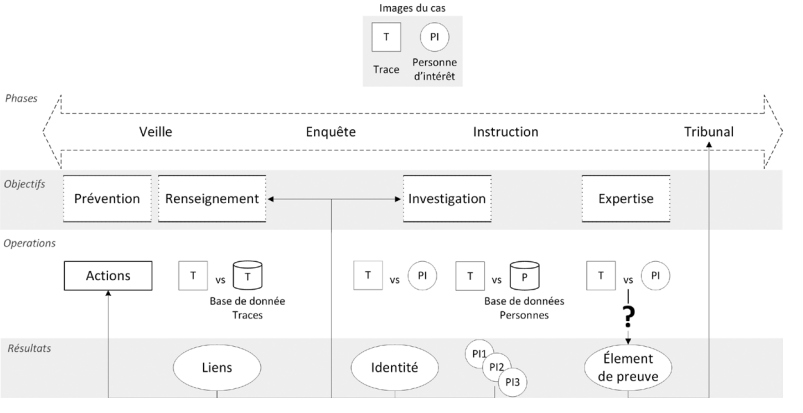
L'utilisation d'images à des fins judiciaires comporte quatre objectifs principaux : l'investigation, le renseignement, l'expertise et l'action de prévention (Figure 2). L'investigation et le renseignement peuvent se servir l'un à l'autre dans un processus itératif, puis la phase d'instruction clôture l'enquête par l'évaluation des éléments de preuve pertinents pour les tribunaux. Dans la phase de veille, l'objectif de prévention tire profit de manière proactive des éléments issus du processus de renseignement de manière à réduire les activités délictueuses ou problématiques. La poursuite de ces objectifs à l'aide de la reconnaissance faciale est actuellement mise en œuvre dans différents domaines d'application, tant au sein de la chaîne pénale au sens strict que de manière plus large en considérant les institutions publiques et privées comme susceptibles de jouer un rôle dans l'action de sécurité.

a. Investigation

Pendant la phase d'enquête, les investigateurs recueillent et exploitent des informations (dont font partie les traces) pour aider à reconstruire

FIGURE 2

Synthèse de l'utilisation forensique actuelle d'images dans l'exemple d'un cas comportant une trace et une personne d'intérêt (PI) (traduite et adaptée de Jacquet et Champod, 2020)



le déroulement de l'événement et retrouver des personnes d'intérêt. Pour un cas donné, où la trace est une image faciale, deux opérations peuvent être effectuées (Figure 2). D'une part, un système automatique compare la trace à de larges bases de données d'images et génère une liste de PI potentielles. D'autre part, lorsque l'enquête s'oriente vers une PI absente des bases de données disponibles, l'opérateur.trice peut comparer l'image-trace avec les photographies de référence de la PI. Enfin, les enquêteur.trices peuvent exploiter seuls les résultats de ces comparaisons – automatiques ou manuelles – ou recouper les informations fournies avec les éléments apportés par d'autres traces.

En pratique, les applications mises en place dans la phase d'investigation sont, par exemple, l'analyse rétroactive de vidéosurveillance à la suite d'un événement délictueux, ou l'analyse proactive d'enregistrements en direct afin de repérer des PI ou des personnes à risque. Ces systèmes de reconnaissance faciale en direct (*live face recognition*/LFR) sont implantés dans différentes grandes métropoles et exploitent de vastes réseaux de CCTV (télévision en circuit fermé) sur la voie publique. Des systèmes LFR ont été testés récemment par le Metropolitan Police Service à Londres (Fussey et Murray, 2019) et par le South Wales Police au Pays de Galles (Davies *et al*., 2018). Là où certains pays et villes ont adopté massivement ces systèmes depuis plusieurs années, comme en Chine ou à Moscou (Grynszpan, 2019), d'autres ont fait machine arrière en les retirant, par exemple à Orlando (États-Unis) en 2018 (Cagle et Ozer, 2018), ou les bannissant légalement comme la ville de Chicago (États-Unis).

b. Renseignement

Parallèlement à l'investigation, la phase de veille opérationnelle consiste notamment à produire des renseignements pour contribuer non seulement à l'enquête, mais surtout au modèle d'action de sécurité (Grossrieder et Ribaux, 2019 ; Hane, 2015 ; Ribaux, 2014). Dans le cadre d'un processus de renseignement criminel opérationnel, des données sont recueillies sur chaque cas, intégrées dans une mémoire, puis analysées afin d'extraire des informations sur le *modus operandi* et les auteur.es. En parallèle, la comparaison d'images-traces de différents cas entre elles aide à repérer des liens entre ces cas, qui étayent l'enquête en cours, et s'intègrent également au suivi systématique de la criminalité répétitive pour détecter, prolonger ou confirmer des séries (Rossy, Ioset, Dessimoz et Ribaux, 2013). Dessimoz et Champod (2015) décrivent un exemple

concret du traitement actuel des images à des fins d'enquête et de renseignement en Suisse, à l'aide d'une plateforme de suivi de la délinquance sérielle et itinérante. Cette étude a permis de constater que le nombre de liens détectés grâce aux images a fortement augmenté de 2009 à 2013, de même que le nombre d'événements associés avec des images. En revanche, ceux associés avec d'autres types de traces (ADN, traces papillaires et traces de semelles) restaient stables (Rossy *et al.*, 2013). Toutefois, les auteurs soulignent le fait qu'en 2013, au moment de la collecte des données, le pourcentage d'images adaptées à l'utilisation des systèmes automatiques était encore très faible (3,2 %). Cette proportion est susceptible d'être revue à la hausse actuellement, compte tenu notamment du fort développement de ces systèmes ces dernières années, tant en termes de performance que de diffusion.

c. Prévention

Les tâches de reconnaissance faciale servent également de manière proactive, notamment eu égard à leur capacité à soutenir des mesures de prévention situationnelle. Issue des approches du même nom en criminologie, la prévention situationnelle réunit ainsi l'ensemble des mesures qui ont pour objectif de prévenir les actes contraires aux normes en limitant les opportunités pour leurs auteur.es de les commettre, par exemple en alourdissant le risque perçu par ces dernier.ières d'être arrêté.es et en réduisant au minimum les avantages escomptés (Jendly, 2013). Parmi les techniques situationnelles synthétisées par Clarke et Eck (2005), la reconnaissance faciale est principalement utilisée pour augmenter les efforts et les risques perçus. Cela se traduit principalement par des contrôles d'accès, sous deux formes pouvant être combinées.

Dans la première forme, le visage des personnes souhaitant accéder à un lieu précis est comparé à une base de données de personnes autorisées. Dans le domaine pénitentiaire par exemple, il s'agit de contrôler les accès des visiteur.es en vue de prévenir les différents trafics au sein de l'établissement pénitentiaire (p. ex. : stupéfiants, téléphones portables, cigarettes, etc.). Au Royaume-Uni, trois prisons ont testé un tel système en 2019 (BBC News, 2019a). Certaines sociétés proposent également des solutions de reconnaissance faciale permettant de localiser et suivre les détenu.es au sein de l'établissement pénitentiaire (FaceFirst, s.d.). À notre connaissance, aucune institution n'a publiquement annoncé recourir à cette utilisation. Dans le domaine de la sécurité

au sens large, de nombreux exemples récents montrent l'intérêt des institutions publiques et privées pour ces technologies. En 2019, deux lycées en France ont testé un tel système pour réguler l'accès à leurs établissements par les élèves. Néanmoins, la Commission nationale de l'informatique et des libertés (CNIL, 2019) a considéré le dispositif projeté comme disproportionné par rapport à l'objectif (contrôle d'accès d'un lycée). Dans le contexte des contrôles aux frontières, plusieurs aéroports aux États-Unis et en France ont mis en place un système permettant de déterminer si les passager.ères sont autorisé.es à pénétrer dans les zones d'embarquement (Métro, 2019).

Dans la seconde forme, les comparaisons sont effectuées avec une base de données de personnes non autorisées à accéder aux lieux. Par exemple, l'identification des hooligans à l'entrée des matchs de football permet de prévenir les violences et dégradations en leur en interdisant l'accès (Woodward, 2001). L'objectif est de prévenir la survenue d'affrontements pendant et à l'issue du match en empêchant les personnes à risque d'entrer. Un principe similaire a été appliqué lors d'un concert de la chanteuse Taylor Swift en 2018 dans le but d'identifier des fans harceleurs (*stalkers*) (BBC News, 2019b).

Au-delà des contrôles d'accès, la reconnaissance faciale a des effets proactifs et dissuasifs liés au renforcement de la surveillance formelle et à la réduction de l'anonymat, par exemple par la présence de télévision en circuit fermé (CCTV) visible sur la voie publique. Cependant, si les méta-analyses sur l'effet des CCTV montrent que la présence de tels systèmes aide à réduire la criminalité contre le patrimoine dans des contextes particuliers (Farrington, Gill, Waples et Argomaniz, 2007 ; Welsh et Farrington, 2009), rien ne permet à l'heure actuelle de démontrer un effet supplémentaire lié à l'ajout de la reconnaissance faciale sur ces CCTV.

d. Expertise

Lorsque cela est requis par l'instruction judiciaire, la finalité de l'expertise forensique est l'interprétation des résultats de comparaisons entre les images-traces et les images de référence afin de les présenter comme élément de preuve au tribunal (Figure 3). Le problème actuel est qu'aucune méthode standardisée ne permet de réaliser cette étape, comme c'est le cas dans les domaines de la reconnaissance de locuteurs (Botti, Alexander et Drygajlo, 2004 ; Meuwly, 2001) et des traces papillaires (Egli, 2009). La technique de comparaison, qu'elle soit

manuelle ou automatisée, doit répondre à des exigences légales très variables selon le pays pour être utilisée devant les tribunaux.

D'une part, en Amérique du Nord, la FRE 702 (Federal Rules of Evidence, 2019) aux États-Unis, issue de la jurisprudence *Daubert v. Merrell Dow Pharmaceuticals* (1993), et la jurisprudence issue de *R v. Mohan* (1994) au Canada, exigent qu'une méthode présentée soit fondée sur une base scientifique fiable et réfutable, qu'elle ait été vérifiée et que les taux d'erreur soient connus, et qu'elle soit disponible pour publication et examen par les pairs. Au Royaume-Uni, d'après *R v. Turner* (1975), l'expertise scientifique doit aller au-delà du bon sens, être fiable[2] et l'expert.e doit posséder les connaissances suffisantes acquises par apprentissage et expérience et faire preuve d'impartialité. Il est néanmoins spécifié que le manque de validation, de publications scientifiques et de révision par les pairs n'est pas rédhibitoire. Enfin, en Europe continentale, il n'existe pas de contrainte légale spécifique au sujet de l'admissibilité de la preuve scientifique, comme décrit dans le Code de procédure pénale du 5 octobre 2007 (art. 182 à 183) en Suisse, et dans le Code de procédure pénale en France (art. 427). Il est seulement précisé que l'expertise doit être justifiée et l'expert.e jugé.e compétent.e dans le domaine requis, et que le/la juge est garant.e de l'évaluation de la pertinence de la preuve en fonction de l'état des connaissances scientifiques.

Pour conclure, il nous apparaît que, malgré les disparités du cadre légal entourant l'expertise scientifique selon les pays, l'emploi de techniques nouvelles doit être soumis à des tests empiriques sur des données adéquates pour garantir de présenter au tribunal des résultats fiables et dont l'expert.e connaît les risques d'erreurs. En outre, un second frein à l'utilisation de ces systèmes est, selon Dessimoz et Champod (2015), la faible qualité des images CCTV. Au contraire, selon Peng (2019), l'exécution de tâches de reconnaissance faciale dépend fortement de la qualité des données d'apprentissage sur lesquelles un système de *machine learning* a été entraîné. Par conséquent, la comparaison d'images de faible qualité nécessite l'utilisation d'un modèle adéquat entraîné sur des données de qualité similaire. Cette étude démontre que les freins actuels à l'utilisation de ces systèmes à des fins évaluatives ne sont pas infranchissables. Nous développons les limitations et perspectives apparentées à ces problématiques dans la section Enjeux liés aux images.

2. Ici, *reliability* regroupe les notions de « validité », « reproductibilité », « justesse » et « répétabilité ».

e. Perception des acteurs

L'usage croissant de ces technologies contraste fortement avec le faible nombre d'études empiriques sur leur efficacité et leur efficience dans leur application pratique. La plupart des sources disponibles concernant l'utilisation de la reconnaissance faciale en matière de sécurité se résument aux articles de presse ou à des rapports de travail institutionnels.

Peu d'études s'attachent à la perception et l'acceptation de ces nouvelles technologies par les différents acteurs qui les emploient soit en tant qu'utilisateurs directs (p. ex. : services de police, tribunaux, etc.), soit en tant que citoyen.nes susceptibles de figurer dans une base de données. Une étude australienne portant sur l'utilisation et l'acceptation des mesures biométriques chez les victimes de vol et d'utilisation frauduleuse de données personnelles montre que plus d'un tiers des répondant.es seraient porté.es à utiliser la reconnaissance faciale comme moyen d'identification, et l'adhésion à cette technologie serait encore plus forte chez les adultes plus âgé.es et les utilisateur.trices régulier.ières d'ordinateurs (Emami, Brown et Smith, 2016). Dans le cadre d'une étude sur la perception des citoyen.nes états-unien.nes de l'utilisation de la reconnaissance faciale des caméras corporelles des policiers, Bromberg, Charbonneau et Smith (2020) montrent que le soutien publiquement affiché par les citoyen.nes est susceptible de diminuer lorsque l'anonymat du/de la répondant.e est assuré. Ils soulignent également l'importance de l'influence sociale dans l'acceptation d'une nouvelle technologie. En plus des caractéristiques sociodémographiques des acteurs, l'adhésion à la reconnaissance faciale est également tributaire de ses objectifs et domaines d'application. Le soutien de la population est par exemple plus important dans le cadre de la protection des frontières (SITA, 2017 ; Unisys Australia, 2014) que lors d'une utilisation en entreprise avec des caméras de vidéosurveillance (Rainie et Duggan, 2016).

Ce bilan permet de dépeindre le cadre opérationnel qui entoure l'utilisation actuelle de la reconnaissance faciale au sein des sciences criminelles et d'en identifier les principales caractéristiques et niveaux d'analyse. Le potentiel de ces utilisations s'observe principalement à travers des cas isolés car il est rarement évalué empiriquement. Parmi les exemples les plus récents se trouve celui de l'auteur d'une tentative de viol dans un métro new-yorkais qui a pu être arrêté grâce à la reconnaissance faciale (Miles, 2020). L'individu était connu des services de police, mais pour des délits sans aucun lien et se trouvait donc dans

une base de données différente, ce qui compliquait son identification. Le système automatique prend tout son sens dans ce type de situation, car il permet d'identifier rapidement un auteur parmi de larges jeux de données que l'humain n'aurait pas pu parcourir entièrement et permet ainsi de prévenir de potentiels futurs délits. Malgré ces résultats prometteurs, à l'heure actuelle le manque d'études empiriques ne permet pas d'évaluer précisément les forces et les faiblesses des systèmes de reconnaissance faciale. D'où la nécessité de mieux situer leurs limitations et enjeux opérationnels ainsi que les perspectives de développement et de recherche que nous jugeons essentiels.

Enjeux et perspectives

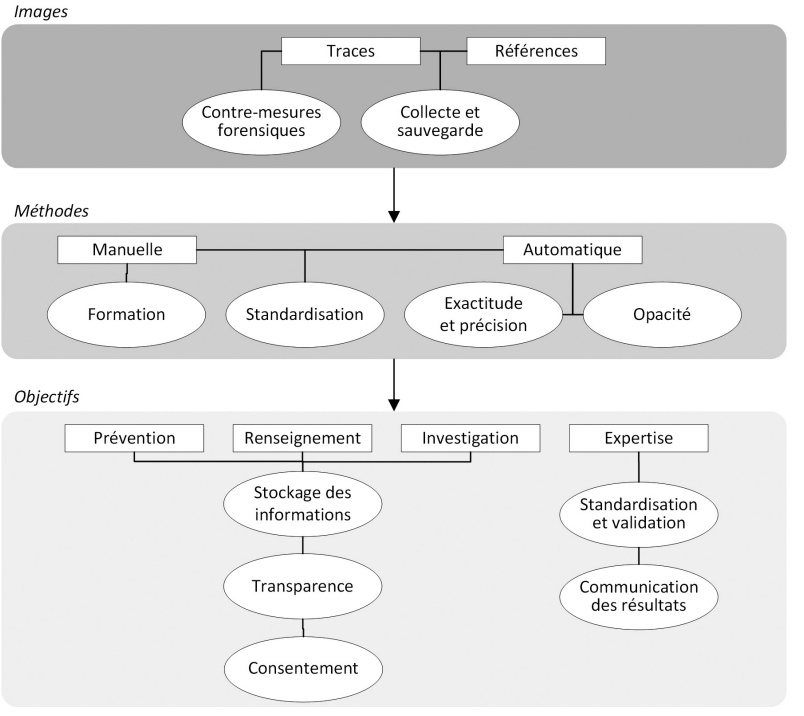
Les enjeux de l'utilisation de la reconnaissance faciale forensique, ainsi que les obstacles rencontrés dans son développement, diffèrent grandement selon le niveau d'analyse. On peut distinguer des enjeux sur trois plans (Figure 3) : les enjeux liés aux images (1), aux méthodes (2), aux objectifs (3).

Enjeux liés aux images

Comme mentionné précédemment, la reconnaissance faciale est présentée à travers les médias, surtout fictionnels, comme un outil « miracle » capable de fournir un résultat irréfutable dans des conditions souvent irréalistes, omettant les facteurs qui influencent l'utilisation des images. En réalité, des facteurs sur deux plans sont susceptibles d'affecter l'utilisation des images dans des tâches de reconnaissance faciale. Tout d'abord, en ce qui a trait à l'activité enregistrée par les outils de capture vidéo, les individus engagés dans des activités délinquantes peuvent masquer leur identité par différents stratagèmes, tels qu'un changement de tenue ou le port de cagoule, de masque, de capuche et de lunettes pour dissimuler leur visage. Ces contre-mesures constituent un des freins majeurs à l'utilisation des images de surveillance dans un but forensique, et il est plus difficile d'intervenir pour réduire cette problématique. Un autre problème récurrent se situe sur le plan de la qualité de l'image fournie aux investigateur.trices. Dans un premier temps, cette qualité est régie par les caractéristiques intrinsèques de l'appareil d'enregistrement (résolution de l'image, colorimétrie, distorsions, etc.) ainsi que par les conditions de prise de vue (luminosité, angle, netteté, etc.).

FIGURE 3

Principaux enjeux de la reconnaissance faciale en sciences criminelles selon le niveau d'analyse



La qualité varie donc considérablement d'une source à l'autre. Par exemple, une photographie de type « selfie » trouvée par le biais de réseaux sociaux, initialement prise avec un appareil à haute résolution, constitue un matériel de meilleure qualité qu'un enregistrement de caméra de vidéosurveillance à résolution moyenne et située en hauteur par rapport à la cible. Néanmoins, une image originale de très bonne qualité, enregistrée à un DAB équipé d'une caméra à haute résolution par exemple, peut être fournie aux investigateurs dans une qualité détériorée. En cause, le format et la manière dont les images sont récoltées, puis partagées.

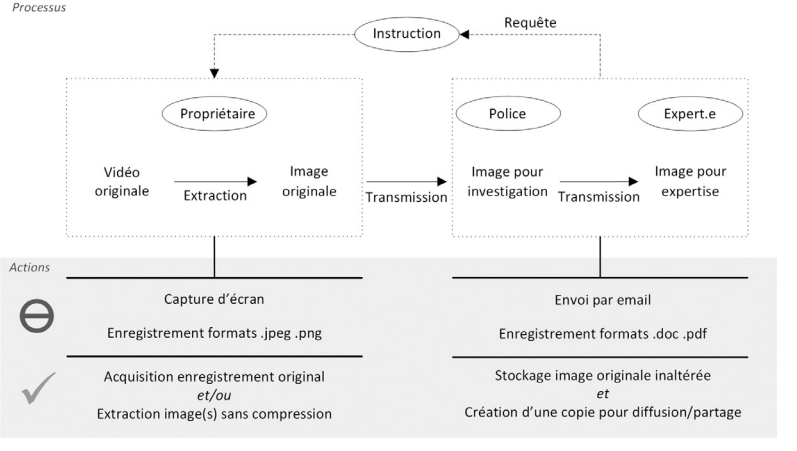
Lors d'une enquête par exemple, les investigateurs prennent connaissance de l'enregistrement de la caméra de surveillance et en demandent l'accès. Idéalement, le propriétaire de l'enregistrement doit fournir le

fichier vidéo original ou, à défaut, une copie de celui-ci sans modification de format ni traitement ou compression. Cependant, dans une grande majorité de cas, les images disponibles sont elles-mêmes des enregistrements de l'image originale. Par exemple, l'investigateur photographie à l'aide d'un téléphone portable l'écran où est affichée l'image originale ou sauvegarde l'image sous un format causant la perte de qualité, tels des fichiers au format PDF ou DOC. Ces pratiques détériorent considérablement la qualité de détails d'intérêt pour l'enquête et, dans les cas où l'investigation débouche sur une procédure nécessitant une expertise, si des images de faible qualité sont fournies à l'expert.e, il/elle devra émettre une demande d'acquisition des images originales au propriétaire par l'intermédiaire du responsable de l'instruction du cas. En l'absence des originaux, l'expert.e peut être amené.e à refuser l'expertise à défaut de matériel de qualité suffisante, ou d'effectuer une expertise dont la fiabilité pourrait être discutée au tribunal. Contrairement à la présence de contre-mesures forensiques lors de l'activité, il est plus aisé d'agir pour améliorer le processus de récolte et de sauvegarde des images-traces. La Figure 4 résume le processus d'acquisition et de transmission des images d'intérêt forensique, et met en évidence les pratiques actuelles à l'origine de leur détérioration ainsi que nos recommandations de solutions de rechange.

Plus précisément, la Figure 5 illustre brièvement l'étendue des variations que provoquent différents modes et formats d'extraction sur le

FIGURE 4

Cheminement et manipulation des images dans le système judiciaire



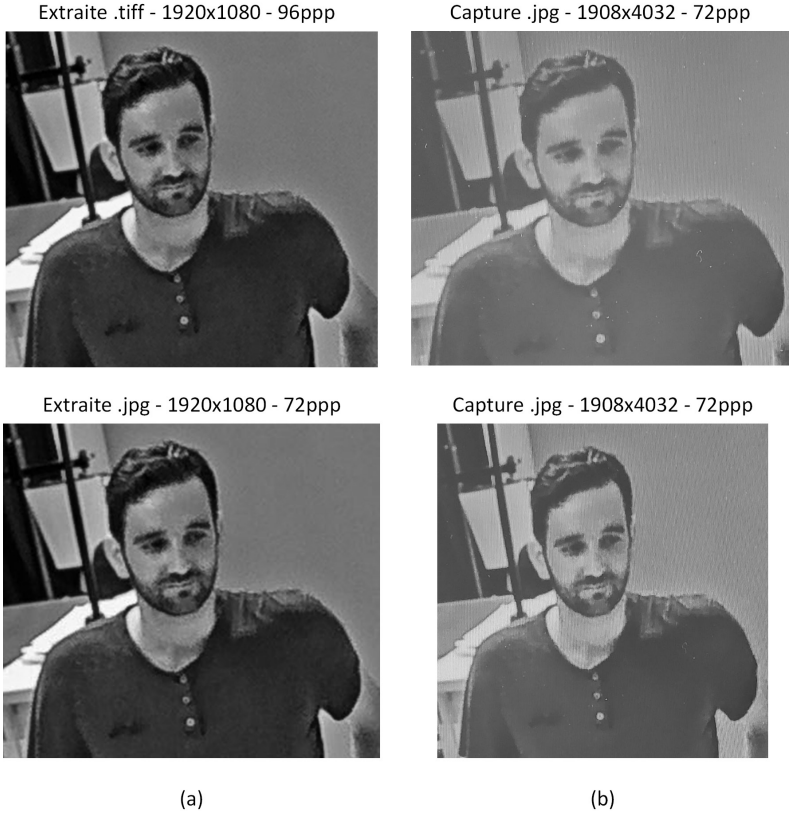
plan de la qualité observable d'une image et de sa résolution. Pour cet exemple, le but était d'enregistrer une image où le visage de la PI est visible, à partir d'une vidéo enregistrée par une caméra de surveillance de haute résolution (1080p). Les deux images (a) ont été extraites à l'aide d'un script Python et du logiciel ouvert VirtualDub, respectivement aux formats TIFF et JPG. Dans les deux cas, la qualité observable de l'image semble similaire, mais la résolution de l'image au format JPG (72 ppp [points par pouce]) est en réalité inférieure. Cette différence, à peine décelable par l'être humain, peut avoir en revanche un impact sur le processus d'analyse du système automatique. Les images (b) résultent de la capture de la même image, mais par l'intermédiaire de l'appareil photo d'un téléphone portable. Il s'agit alors de photographies au format JPG de l'image d'intérêt. Bien que la résolution soit comparable à celle de l'image JPG extraite (a), la qualité globale de l'image est très visiblement détériorée. De plus, ces deux captures ont été prises avec le même appareil, par le/la même opérateur.trice, dans des conditions similaires et à quelques secondes d'intervalle l'une de l'autre. Malgré cela, la présence et l'intensité des distorsions sont indéniables et diminuent considérable l'image d'intérêt. Il est également à noter qu'il ne s'agit ici que de variations survenant à l'étape d'extraction du matériel original, et que ces détériorations peuvent par la suite s'accumuler avec la multiplication d'étapes de transmission et de stockage de cette même image par les différents acteurs judiciaires (Figure 4). Malheureusement, comme exposé précédemment, les images-traces collectées par les forces de l'ordre sont très rarement extraites de manière optimale, le plus souvent dans un souci de simplification et de gain de temps. Par exemple, la plateforme intercantonale d'échange d'informations liées aux cas de Suisse latine[3] (Dessimoz et Champod, 2015) contient exclusivement des images stockées aux formats JPG et BMP, dont les taille, résolution et mode de capture sont très variables.

Ces pratiques courantes impactent par la suite tous les processus d'analyse et de comparaison, et peuvent nécessiter une requête pour l'acquisition du matériel original auprès du propriétaire, par le biais de l'instruction chargée du cas. Cela peut être imputé en grande partie à l'utilisation encore récente de détails tels que le visage dans les images récoltées, aggravé par la perception souvent trop simpliste sur ces technologies, véhiculé par les médias, comme discuté précédemment.

3. La Suisse « latine » regroupe tous les cantons de Suisse romande et le Tessin.

FIGURE 5

Illustration des variations de qualité visuelle et de résolution d'images (a) extraites et (b) capturées à l'aide d'un téléphone portable (Samsung S10) à partir d'une vidéo de caméra de surveillance (AXIS P3245-V)



En l'absence de sensibilisation adéquate pour tous les acteurs intervenant sur l'ensemble des processus de collecte et transmission d'images, ces derniers sont plus enclins à baser leurs pratiques sur cette vision erronée de systèmes de reconnaissance faciale tout-puissants, capables de reconnaître un individu à partir de vidéos pixellisées d'une PI prise de profil, par exemple. De plus, dans un objectif évaluatif, les exigences se multiplient, comme expliqué dans la section dédiée, alors que les images fournies lors des demandes d'expertises sont souvent celles déjà collectées et transmises de manière inadéquate.

Enjeux liés aux méthodes

L'amalgame récurrent entre la complexité et l'efficacité d'un système se traduit auprès des décideurs par un besoin d'un système à la pointe de la technologie et supposé onéreux. Au contraire, cette impression de complexité est rarement synonyme d'efficacité et soulève plusieurs enjeux.

a. Opacité des systèmes automatiques

Selon Burrell (2016), l'opacité des algorithmes peut être intentionnelle à des fins commerciales ou sécuritaires, mais elle peut découler aussi du niveau de compétence à avoir pour les comprendre ou de la manière dont les algorithmes fonctionnent au sein du système entier. Cet effet boîte noire (*blackbox)* (Pasquale, 2015) et le manque de connaissances sur leur fonctionnement sous-jacent sont un frein à leur optimisation et donc à leur performance. Parmi les effets problématiques générés, le plus régulièrement rapportés dans la presse pour les répercussions désastreuses évidentes que ceux-ci peuvent induire est celui du biais racial. Le processus d'apprentissage, essence du fonctionnement du *machine learning,* permet d'entraîner un algorithme à reconnaître des visages sur de très larges bases de données. Le problème est qu'en utilisant une majorité d'images faciales de personnes de type caucasien comme c'est le cas aujourd'hui, l'algorithme ne sait pas aussi bien reconnaître les visages de type ethnique différent, p. ex. : afro-américain. Cela représente un problème majeur pour l'utilisation opérationnelle de ces algorithmes dans un grand nombre de pays où la population regroupe de nombreuses origines ethniques différentes. Une solution serait donc d'utiliser des bases de données d'apprentissage plus éclectiques, mais il existe encore peu de telles bases en accès libre et assez larges pour garantir un apprentissage performant. La base de données RFW (*Racial Faces in the Wild*) a été créée récemment en réponse à cette problématique (Wang, Deng, Hu, Tao et Huang, 2019).

b. Besoins de standardisation

Les systèmes automatiques apportent de nombreux bénéfices, tant par leurs performances que par leur rapidité d'exécution. Cependant, il n'existe à ce jour aucun guide méthodologique dédié aux expertises en reconnaissance faciale assistées par un système automatique. Chaque système génère un résultat de comparaison selon sa propre méthode, le

plus souvent sous la forme d'un score, et qui doit être « traduit » avant d'être présenté devant un tribunal. Par exemple, l'algorithme *open source* Facenet (Sandberg, 2018) génère des scores entre 0 et 3 représentant la distance – c.-à-d. le degré de dissimilarité – entre deux images, alors que les systèmes commerciaux MorphoFace (Idemia) produisent des scores de similarité entre 0 et 50'000. Les performances exposées dans les rapports FRVT du NIST (Grother *et al.*, 2019) peuvent justifier l'utilisation de certains systèmes par un expert au tribunal, mais il faut noter que ces tests recourent à de larges bases de données collectées dans un but de recherche, souvent peu représentatives des données réelles, ou déjà exploitées pour la phase d'apprentissage, ce qui surestime les performances de l'algorithme qui travaille sur le matériel sur lequel il s'est formé. Il est actuellement toujours nécessaire de conduire des études basées sur des données d'intérêt forensique reflétant au mieux les conditions réelles, et de produire un modèle permettant de « traduire » les différents scores de comparaison pour présenter un résultat fiable de manière standardisée au tribunal.

Ce manque de standardisation n'est plus uniquement un débat de niche réservé aux spécialistes forensiques. En 2019, le tribunal de Lyon a été confronté à un cas inédit en France, dans lequel le seul élément de preuve disponible dans un procès pour vol était un enregistrement de vidéosurveillance. Le résultat de l'expertise en reconnaissance faciale, effectuée à l'aide d'un système automatique, soutenait la proposition de la partie accusatrice. L'avocat de la défense dénonce alors dans les médias l'utilisation de ce « robot accusateur » (Perruche, 2019), en insistant sur le manque de bases scientifiques validées de cette méthode. Cet exemple résume à lui seul la précarité de la situation actuelle de la reconnaissance faciale automatique dans le domaine judiciaire et le besoin de fondations empiriques solides pour consolider la fiabilité de telles expertises.

c. Précision et exactitude

Un dernier enjeu méthodologique consiste à trouver l'équilibre entre les taux de faux positifs (une personne reconnue à tort) et de faux négatifs (une personne exclue à tort) servant le mieux l'objectif final du dispositif de reconnaissance faciale. Ces taux d'erreurs sont essentiels à l'évaluation de la robustesse d'une méthode (Dror, 2020) et sont interdépendants, de telle manière que la calibration d'une méthode visant à diminuer le taux de faux négatifs augmente inexorablement le taux de faux positifs en contrepartie, et inversement.

Par exemple, dans le cadre d'une veille opérationnelle en renseignement visant à repérer un.e suspect.e potentiel.le, la priorité est de s'assurer de ne pas manquer un.e suspect.e potentiel.le (faux négatif), au risque de considérer à tort d'autres personnes (faux positifs). En revanche, dans le cadre de l'évaluation d'éléments de preuve en vue de leur présentation au tribunal, il est essentiel de limiter le taux de faux positifs, car il traduit le risque de condamner une personne à tort.

Parmi les mesures de performance, la précision[4] se reporte à la probabilité que deux images représentent effectivement la même personne lorsque la méthode produit un résultat positif, et l'exactitude[5] est la probabilité de fournir un résultat positif en comparant deux images de la même personne. Malgré la complémentarité de ces deux notions, la performance d'une méthode est souvent réduite à sa précision. Or, bien qu'une méthode extrêmement précise produisant très peu de résultats positifs incorrects paraisse satisfaisante, le fait qu'elle puisse omettre un taux élevé de résultats positifs corrects peut avoir un impact négatif lors de son application.

Enjeux liés aux objectifs

L'idée de systèmes entièrement automatiques et généralisables, véhiculée par les stratégies commerciales et les représentations médiatiques, occulte les spécificités et enjeux propres aux différents objectifs poursuivis en matière de sécurité. Nous distinguons deux types d'enjeux : ceux liés au renseignement, à l'investigation et à la prévention, et ceux liés à l'expertise.

a. Prévention, renseignement et investigation

Comme décrit précédemment, les applications de la reconnaissance faciale à des fins de prévention, renseignement et d'investigation sont principalement dédiés à l'identification de personnes ou à leur supervision dans une séquence vidéo. La poursuite de ces objectifs implique deux conséquences : la nécessité de disposer de bases de données d'images et le déploiement de dispositifs sur l'espace public. Ces conséquences soulèvent alors un certain nombre d'enjeux qu'il s'agit de considérer.

4. Cette notion est comparable à la fiabilité en psychométrie.
5. Cette notion est comparable à la validité en psychométrie.

Tout d'abord, la manière dont est construit et organisé le stockage des données utilisées par les systèmes de reconnaissance faciale a des impacts sur leur application (Marzouki, 2001). Parmi les caractéristiques liées au stockage, l'enjeu principal se situe sur le plan des critères d'inclusion dans la base de données. Ceci est d'autant plus problématique dès lors que le dispositif de reconnaissance faciale est utilisé par les services de police. Ces critères peuvent être plus ou moins larges selon leur compréhension. Par exemple si l'un des critères est d'être une personne recherchée par la police et la justice pour figurer dans la base de données, la limite pourrait être fixée aux personnes sous mandat d'arrêt. Mais cette délimitation peut s'avérer plus large si cela concerne également les personnes suspectées d'un crime sous la seule décision d'un enquêteur (Fussey et Murray, 2019). En allant encore plus loin, des personnes considérées comme étant à risque sans implication dans un délit sont susceptibles d'être incluses. Les tests menés au Pays de Galles (Davies *et al*., 2018) incluent une base de données qui catégorise les personnes en trois niveaux selon le degré d'intérêt de la police et les risques perçus envers la société. En plus des critères d'inclusion, le croisement des images avec d'autres sources d'information, notamment étatiques, peut poser de sérieux dangers en matière de protection des données et de respect de la sphère privée.

Contrairement à d'autres mesures biométriques, le consentement nécessaire à la collecte de données est très difficile à obtenir lors de l'utilisation de la reconnaissance faciale dans les espaces publics (Castelluccia et Le Métayer, 2019). Le consentement peut intervenir à deux moments distincts : à l'étape de capture (enrôlement), c'est-à-dire au moment où l'image de la personne est enregistrée, et à l'étape de comparaison entre deux ou plusieurs images (reconnaissance) (Marzouki, 2001). Au moment de l'enrôlement, le dispositif nécessite la présence de la personne, mais pas d'action de sa part pour enregistrer son visage, à l'inverse par exemple de dispositifs utilisant la reconnaissance par empreinte digitale. Ainsi, la capture du visage peut être prise à l'insu de la personne. En termes de protection des données et de la sphère privée, il s'agit là d'un enjeu majeur. L'information à l'aide d'affiches indiquant la présence de caméra et de dispositifs de reconnaissance faciale ne peut en elle seule suffire comme mode de consentement. En effet, le consentement nécessite un choix libre et éclairé. La pose de panneaux est une information passive, c'est-à-dire que la personne est susceptible de ne pas avoir connaissance de sa présence. De plus, même

en ayant connaissance de la présence du dispositif, il est difficile de connaître son étendue, le champ de vision des caméras étant inconnu. La notion de choix est également mise à mal dès lors que l'alternative est de ne pas se rendre dans la zone concernée. Du moment que le dispositif de reconnaissance faciale est actif dans un espace public, un consentement total devrait permettre aux citoyens des moyens alternatifs de continuer leur chemin sans emprunter la zone couverte par les caméras. Le refus de consentement en évitant les zones surveillées ou en se masquant le visage est également susceptible d'entraîner des réactions de suspicion de la part des forces de l'ordre dès lors que ces actions peuvent découler d'un effet préventif provoqué par le dispositif (Fussey et Murray, 2019). La question du consentement s'inscrit de manière plus large dans la transparence liée au dispositif. De manière similaire à l'effet boîte noire qui entoure les algorithmes automatiques, une certaine opacité entoure les dispositifs qui font appel à la reconnaissance faciale, notamment en termes de processus. La transparence peut être alors comprise comme le degré d'information à la disposition du public, notamment concernant l'utilisation du système de reconnaissance faciale, ses objectifs, ses localisations et son fonctionnement. Cette transparence joue un rôle important dans la perception de la légitimité du dispositif, et dans le contrôle (*accountability*) des acteurs qui le gèrent (services de police, sécurité privée, etc.) (Fussey et Murray, 2019). L'enjeu se situe alors sur deux plans : (i) déterminer la quantité d'information à mettre à disposition des citoyens sans compromettre l'utilité opérationnelle du dispositif et (ii) impliquer activement la société civile tant dans la conception que la mise en œuvre des dispositifs de reconnaissance faciale dans les espaces publics. Ces différents enjeux liés à la reconnaissance faciale dans la prévention, le renseignement et l'investigation gravitent autour des libertés individuelles, notamment en termes de protection de données et du respect de la sphère privée. Plus encore, ils renvoient à une application biopolitique telle que la conçoit Foucault (1975) dès lors que le noyau dur de l'identité d'une personne, c.-à-d. son visage, fait figure de ressources malléables dans l'exercice d'un pouvoir tant étatique que privé. Malgré les risques générés, des recommandations à destination des services publics sont susceptibles de limiter ces risques et de guider la mise en œuvre de la reconnaissance faciale dans le contexte d'action de sécurité (Castelluccia et Le Métayer, 2019 ; Dupont, Stevens, Westermann et Joyce, 2018) :

- Garantir l'accès au code source et aux algorithmes, afin d'éviter le phénomène de boîte noire ;
- Garantir l'accès aux données utilisées pour entraîner le système de reconnaissance faciale pour éviter les biais de discrimination ;
- Mettre en place des mesures de contrôle pour répondre à l'enjeu de transparence ;
- Évaluer la pertinence (adéquation), l'efficacité (effet) et l'efficience (coût-bénéfice) du dispositif ;
- Évaluer l'impact de l'adoption de systèmes de reconnaissance faciale tant sur les usager.ères que les professionnel.les pour faciliter leurs intégration et acceptation au sein de la société civile.

b. Expertise

La reconnaissance faciale automatique est de plus en plus largement étudiée au moyen de problématiques techniques et statistiques (Li et Jain, 2009 ; Tistarelli et Champod, 2017) ainsi que dans le domaine du renseignement forensique (Dessimoz et Champod, 2015). Cependant, il n'existe pas encore de méthode évaluative qui réponde intégralement aux besoins judiciaires dans le domaine de la reconnaissance faciale, comme c'est le cas dans les domaines de la reconnaissance de locuteurs (Botti *et al.*, 2004 ; Meuwly, 2001) et des traces papillaires (Egli, 2009).

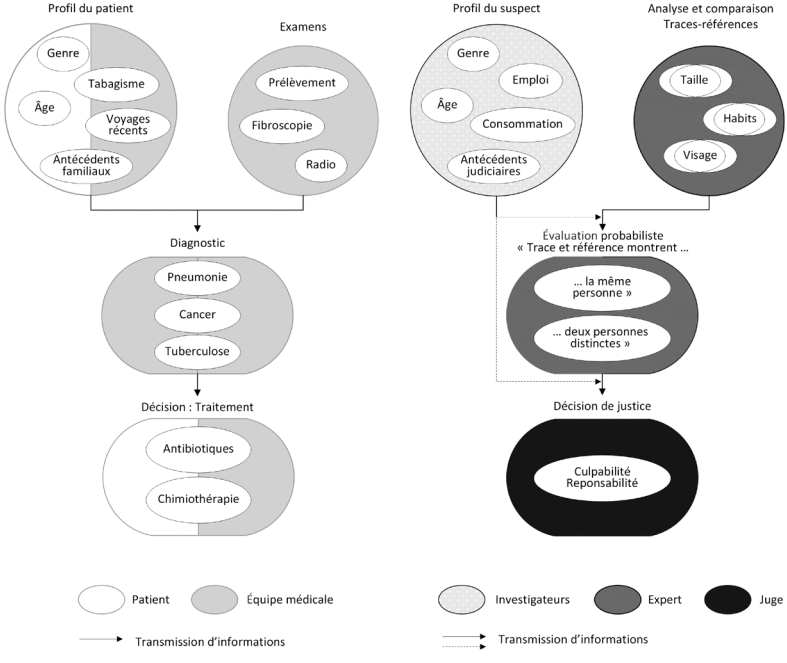
Au tribunal, la communication entre experts, juristes et jurés pâtit du manque de jargon commun à tous les protagonistes, qui possèdent chacun leurs propres codes adaptés à leurs objectifs et domaines de connaissances. Néanmoins, un procès nécessite de réunir toutes les informations disponibles de manière pertinente pour alimenter efficacement la discussion autour d'un seul et même événement d'intérêt.

Le processus le plus utilisé par les expert.es pour l'exploitation de traces d'intérêt forensique suit une phase d'analyse des traces et références fournies, puis on procède à leur comparaison et, enfin, à l'évaluation des résultats. Compte tenu de la complexité de la tâche allouée à l'expert.e et de son rôle au sein du système judiciaire, celui/celle-ci ne peut pas exprimer le résultat de la comparaison de deux images en concluant à une identification – ou exclusion – en fonction d'un seuil fixé, à la manière d'un système autorisant l'accès à un bâtiment. Dans cette optique, l'une des solutions les plus étudiées par les forensicien.nes est la méthode probabiliste, qui permet de donner un poids au

résultat d'une comparaison en regard de propositions[6] mutuellement exclusives, qui retranscrivent les points de vue des deux parties engagées dans le procès (Robertson, Vignaux et Berger, 2016). Afin d'appréhender plus concrètement le principe de cette approche, nous proposons un parallèle de son application dans les processus médical et judiciaire (Figure 6). Il est important de préciser que cette comparaison vise à illustrer le processus de prise de décision dans le cadre de la justice grâce à un domaine que nous jugeons plus concret et répandu et dont le processus décisionnel est comparable, sans être identique. La description du processus médical repose sur un exemple simple dont la description ne se veut en aucun cas exhaustive.

FIGURE 6

Parallèle entre les processus de décision et la transmission d'informations entre acteurs dans les domaines médical (gauche) et judiciaire (droite)



6. Le terme « propositions » se réfère aux hypothèses de travail dans le cadre précis de l'évaluation forensique.

La partie gauche de la Figure 6 présente un exemple de processus médical basé sur le modèle interprétatif (Gerber, Kraft et Bosshard, 2014), de l'apparition de symptômes à la prise de décision concernant le traitement à utiliser. Un.e patient.e se présente avec plusieurs symptômes tels que de la fièvre, une toux persistante et des douleurs thoraciques. Le/la médecin établit un profil du/de la patient.e afin de pouvoir déceler d'éventuels antécédents et facteurs de risque. En complément, des examens sont effectués pour apporter des informations supplémentaires quant aux symptômes et à leurs causes potentielles. Les informations *a priori* composant le profil du/de la patient.e et les résultats d'examens sont évalués par le/la praticien.ne afin d'orienter son diagnostic vers la pathologie la plus probable parmi les causes envisagées. Ce diagnostic lui permet alors de prendre une décision quant au traitement le plus adapté.

Dans un tel cas, il est courant que le/la médecin informe le/la patient.e de sa décision finale sans détailler les probabilités qui ont pu entrer en considération dans le processus. Le/la patient.e se repose alors entièrement sur l'expérience de son interlocuteur.trice et donne son accord. Si ce processus permet de diagnostiquer un cancer avec une probabilité de 95 %, le/la médecin peut prescrire rapidement une chimiothérapie, avec un faible risque d'erreur et donc de répercussion néfaste sur le/la patient.e. Cependant, si le diagnostic s'oriente à 60 % vers un cancer, et à 40 % vers une autre pathologie, le risque de faire subir une chimiothérapie non nécessaire au/à la patient.e, avec les effets néfastes qu'un tel traitement implique, est significativement plus élevé. Le/la médecin peut-il/elle alors toujours être seul·e décisionnaire ou devrait-il/elle en référer à d'autres professionnel.les du corps médical ou au/à la patient.e au préalable ? [7]

Dans le domaine forensique, le processus décisionnel est plus fragmenté et moins linéaire, comme illustré par la partie droite de la Figure 6. Les informations *a priori* proviennent de l'enquête menée par les investigateurs des forces de l'ordre sur un.e suspect.e. Ces informations ne sont pas nécessairement fournies (volontairement ou non[8]) au/à la

7. La méthode de prise de décision partagée entre médecins et patient,es est toujours vivement discutée par les praticien.nes depuis une vingtaine d'années, parmi plusieurs autres méthodes (Fried, 2016 ; Gerber *et al.*, 2014).

8. La question de la communication ou non des informations d'enquête aux expert.es n'est pas triviale et demeure sujette à controverse parmi les forensicien.nes. Il peut être considéré que la connaissance de telles informations risque d'orienter, consciemment ou

forensicien.ne chargé.e de l'expertise des images liées au cas. L'analyse des traces, c.-à-d. les images prises pendant les faits, permet de déterminer les éléments d'intérêt à comparer au matériel de référence, c.-à-d. des photographies du/de la suspect.e. Par exemple, la taille de l'individu, ses vêtements et son visage sont des éléments communément exploités dans la comparaison d'images lors d'expertise forensique. Une fois la comparaison – manuelle ou automatique – effectuée, l'évaluation probabiliste des résultats permet de donner plus ou moins de poids à l'une ou l'autre des propositions définies à l'aide des parties engagées dans la procédure :

- Proposition de l'accusation : La trace et la référence montrent la même personne, le/la suspect.e.
- Proposition de la défense : La trace et la référence montrent deux personnes différentes, le/la suspect.e et un autre individu.

L'expert.e communique donc la conclusion de son évaluation au tribunal, auquel sont également fournies les informations *a priori* du/de la suspect.e par les investigateur.trices. Il appartient alors au/à la juge de prendre la décision finale, concernant la culpabilité et la responsabilité du/de la suspect.e, en prenant en compte à la fois les conclusions de l'expertise et les informations *a priori*, et d'adapter la peine en adéquation avec sa décision.

Pour revenir au parallèle dans le domaine médical, le choix d'informer ou non le/la patient.e des probabilités ayant orienté la décision du traitement à recommander appartient au/à la médecin. Celui/celle-ci joue un rôle dans chaque étape du processus, jusqu'à la décision finale, qu'il/elle peut partager avec le/la patient.e dans certains cas. Dans le système judiciaire, ce rôle transversal n'existe pas. Ce domaine réunit un grand nombre d'acteurs, aux professions, jargons, mais également objectifs différents, autour d'un même cas, et le/la suspecte ne peut nullement intervenir à la manière d'un.e patient.e. De même, l'expert.e ne peut pas se prononcer sur la décision finale. Il est donc essentiel d'optimiser les moyens de communication pour garantir une prise de décision efficace basée sur une collecte exhaustive des informations de chacun.e.

---

non, l'expertise du/de la forensicien.ne en ayant pris connaissance. D'un autre côté, des informations contextuelles peuvent affiner les hypothèses de travail.

Conclusion

Avec le développement croissant des algorithmes automatiques et de l'intelligence artificielle, la reconnaissance faciale occupe une place toujours plus importante dans un contexte d'action de sécurité et dans la société en général. Cependant, la plupart des sources disponibles concernant son utilisation se résument aux articles de presse ou à des rapports de travail institutionnels. Il existe une réelle lacune en matière d'études empiriques sur les différentes utilisations de ces technologies en sciences criminelles et sur la perception de celles-ci par les acteurs qui les mettent en œuvre. Les potentiels effets apportés en matière de prévention, de renseignement, d'investigation et d'expertise sont accompagnés d'enjeux et de limites qu'il s'agit de considérer, au risque de compromettre une mise en œuvre adéquate de dispositifs de reconnaissance faciale, dont la nature protéiforme en fait un objet-frontière entre la criminologie et la science forensique. Ainsi, l'état des lieux proposé dans cet article a comme ambition de fournir un cadre de travail interdisciplinaire structuré afin d'orienter les perspectives de recherches essentielles dans ce domaine. Comme démontré, il est crucial de comprendre et de délimiter les enjeux qui diffèrent fortement selon le niveau d'analyse considéré. Les enjeux liés aux images et aux méthodes impactent l'ensemble des différentes applications dès lors qu'elles constituent la base de la reconnaissance faciale. À l'inverse, les enjeux liés aux objectifs se révèlent beaucoup plus spécifiques. Approfondir ce champ d'études est d'autant plus important que la mise en place d'un dispositif de reconnaissance faciale pour l'action de sécurité est susceptible d'être étendue à d'autres fins, notamment en termes de prévention sanitaire. La crise liée à la pandémie de COVID-19 en 2020 est un parfait exemple. À Moscou et en Chine, la reconnaissance faciale est combinée avec les mesures de température et la localisation pour tenter d'identifier des malades potentiels (Salas, 2020). Bien entendu, de nombreuses problématiques accompagnent ces évolutions et la crainte de voir émerger une version 2.0 du panoptique de Bentham et de la disciplinarisation des corps de Foucault est bien présente. Plutôt que de céder à une diabolisation de cette technologie et arriver à des extrêmes tels que le bannissement total, nous préconisons de réguler sa mise en œuvre et surtout de fournir les clés de sa compréhension et de son utilisation tant en ce qui concerne les acteurs qui la déploient que ceux qui l'éprouvent. « Le pouvoir du panoptique [peut ainsi être] limité par le processus consistant à donner aux personnes observées un degré de

contrôle et de connaissances des systèmes de reconnaissance faciale » (Gray, 2003).

Références

Ali, T., Veldhuis, R. et Spreeuwers, L. (2012). Forensic face recognition : A survey. Dans A. Quaglia et C. M. Epifano (dir.), *Face recognition : Methods, applications and technology* (p. 9-28). Nova Publishers.

BBC News. (2019a, 6 mars). Prison visitors get face recognition scans in drug crackdown. Repéré à https://www.bbc.com/news/uk-47461035

BBC News. (2019b, 10 septembre). Musicians call for facial recognition ban at gigs. Repéré à https://www.bbc.com/news/technology-49647244

Bertillon, A. (1886). De l'identification par les signalements anthropométriques. *Archives de l'anthropologie criminelle et des sciences pénales*, *1*, 193-223.

Botti, F., Alexander, A. et Drygajlo, A. (2004). An interpretation framework for the evaluation of evidence in forensic automatic speaker recognition with limited suspect data. *ODYSSEY 2004 – The Speaker and Language Recognition Workshop*, 63-68.

Bromberg, D. E., Charbonneau, É. et Smith, A. (2020). Public support for facial recognition via police body-worn cameras : Findings from a list experiment. *Government Information Quarterly*, *37*(1), 101415. https://doi.org/10.1016/j.giq.2019.101415

Buchanan, B. G. (2005). A (very) brief history of artificial intelligence. *AI Magazine*, *26*(4), 53-53. https://doi.org/10.1609/aimag.v26i4.1848

Burrell, J. (2016). How the machine 'thinks' : Understanding opacity in machine learning algorithms. *Big Data & Society*. https://doi.org/10.1177/2053951715622512

Cagle, M. et Ozer, N. (2018). *Amazon teams up with government to deploy dangerous new facial recognition technology*. American Civil Liberties Union. Repéré à https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazon-teams-government-deploy-dangerous-new

Castelluccia, C. et Le Métayer, D. (2019). *Analyse des impacts de la reconnaissance faciale Quelques éléments de méthode*. Grenoble, France : Inria Grenoble Rhône-Alpes.

Clarke, R. V. et Eck, J. E. (2005). *Crime analysis for problem solvers in 60 small steps*. Washington, DC : Center for Problem Oriented Policing.

Cole, S. A. et Dioso-Villa, R. (2007). CSI and its effects : Media, juries, and the burden of proof. *New England Law Review*, *41*, 435-469.

Commission Nationale de l'Informatique et des Libertés. (2019). *Expérimentation de la reconnaissance faciale dans deux lycées : La CNIL précise sa position*. Repéré àhttps://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position

Committee on Facilitating Interdisciplinary Research. (2004). *Facilitating Interdisciplinary Research*. Washington, DC : The National Academy Press. Repéré à http://www.nap.edu/catalog/11153/facilitating-interdisciplinary-research

Davies, B., Innes, M. et Dawson, A. (2018). *An Evaluation of South Wales Police's Use of Automated Facial Recognition*. Universities' Police Science Institute, Crime and Security Research Institute, Cardiff University, Royaume-Uni.

Dessimoz, D. et Champod, C. (2015). A dedicated framework for weak biometrics in forensic science for investigation and intelligence purposes : The case of facial information. *Security Journal*, *29*(4), 603-617. https://doi.org/10.1057/sj.2015.32

Dror, I. E. (2020). The error in "error rate" : Why error rates are so needed, yet so elusive. *Journal of Forensic Sciences*, *65*(4), 1034-1039. https://doi.org/10.1111/1556-4029.14435

Dupont, B. (2016). Des effets perturbateurs de la technologie sur la criminologie. *Revue Internationale de Criminologie et de Police Technique et Scientifique*, *69*(3), 305-322.

Dupont, B., Stevens, Y., Westermann, H. et Joyce, M. (2018). *Artificial intelligence in the context of crime and criminal justice*. Korean Institute of Criminology.

Egli, N. (2009). *Interpretation of partial fingermarks using an automated fingerprint identification system* (Thèse de doctorat inédite). Université de Lausanne.

Emami, C., Brown, D. R. et Smith, D. R. G. (2016). Use and acceptance of biometric technologies among victims of identity crime and misuse in Australia. *Trends & Issues in Crime and Criminal Justice*, *511*, 6.

European Network of Forensic Science Institutes. (2018). *Best practice manual for facial image comparison (ENFSI-BPM-DI-01)*.

FaceFirst. (s. d.). Face recognition for correctional facilities. Repéré à https://www.facefirst.com/industry/correctional-facility-face-recognition/

Facial Identification Scientific Working Group. (2012). *Guidelines for Facial Comparison Methods*.

Farrington, D. P., Gill, M., Waples, S. J. et Argomaniz, J. (2007). The effects of closed-circuit television on crime : Meta-analysis of an English national quasi-experimental multi-site evaluation. *Journal of Experimental Criminology*, *3*(1), 21-38. https://doi.org/10.1007/s11292-007-9024-2

Foucault, M. (1975). *Surveiller et punir*. Paris, France : Gallimard.

Fried, T. R. (2016). Shared decision making—Finding the sweet spot. *New England Journal of Medicine*, *374*(2), 104-106. https://doi.org/10.1056/NEJMp1513686

Fussey, P. et Murray, D. (2019). *Independent report on the London Metropolitan Police Service's trial of live facial recognition technology* (The Human Rights, Big Data and Technology Project). Human Right Center, University of Essex, Royaume-Uni.

Gerber, M., Kraft, E. et Bosshard, C. (2014). Décision partagée – Médecin et patient décident ensemble. *Bulletin des médecins suisses*, *95*(50), 1883-1889.

Gray, M. (2003). Urban surveillance and panopticism : Will we recognize the facial recognition society ? *Surveillance & Society*, *1*(3), 314-330. https://doi.org/10.24908/ss.v1i3.3343

Grossrieder, L. et Ribaux, O. (2019). Towards forensic whistleblowing ? From traces to intelligence. *Policing : A Journal of Policy and Practice*, *13*(1). https://doi.org/10.1093/police/pax039

Grother, P., Ngan, M. et Hanaoka, K. (2019). *Face Recognition Vendor Test (FRVT) Part 2 : Identification* (National Institute of Standards and Technology – NIS-TIR 8238).

Grynszpan, E. (2019, 6 mars). Moscou opte pour la surveillance totale à la chinoise. Le temps. Repéré à https://www.letemps.ch/monde/moscou-opte-surveillance-totale-chinoise

Hane, T. (2015). La veille, une autre forme d'acquisition et de mise en valeur de l'information. Dans *L'intelligence économique au service de la lutte contre le blanchiment de capitaux et le financement du terrorisme* (p. 250-269). Université de Strasbourg. https://doi.org///doi.org/10.1016/j.forsciint.2019.110124 https://doi.org/10.1016/j.forsciint.2011.06.023

ISO/IEC 2382-37 : 2017(E). (2017). *Information technology—Vocabulary -Part 37 : Biometrics (ISO/IEC 2382-37 : 2017(E))*. International Organization for Standardization.

Jacquet, M. et Champod, C. (2020). Automated face recognition in forensic science : Review and perspectives. *Forensic Science International*, *307(110124)*.

Jendly, M. (2013). *Prévenir la criminalité : Oui… Mais comment ?* Charmey, Suisse : Les Éditions de l'Hèbe.

LeCun, Y., Bengio, Y. et Hinton, G. (2015). Deep learning. *Nature*, *521*(7553), 436-444. https://doi.org/10.1038/nature14539

Li, S. Z. et Jain, A. K. (2009). *Encyclopedia of Biometric*. New York, NY : Springer Science+Business Media, LLC.

Marzouki, M. (2001). *Enjeux des techniques de biométrie – Une première approche*. Paris, France : CNIL, Association IRIS (Imaginons un réseau Internet solidaire).

Métro. (2019, 18 octobre). La reconnaissance faciale arrive dans les aéroports. Repéré à https://journalmetro.com/techno/2389332/la-reconnaissance-faciale-arrive-dans-les-aeroports/

Meuwly, D. (2001). *Reconnaissance de locuteurs en sciences forensiques : L'apport d'une approche automatique* (Thèse de doctorat inédite). Université de Lausanne.

Miles, F. (2020, 30 août). NYPD uses facial recognition to arrest brazen sex offender accused of attempted rape on subway platform. *Fox News*. Repéré à https://www.foxnews.com/us/nypd-uses-facial-recognition-to-arrest-brazen-sex-offender-accused-of-attempted-rape-on-subway-platform

Moreton, R. et Morley, J. (2011). Investigation into the use of photoanthropometry in facial image comparison. *Forensic Sci Int*, *212*(1-3), 231-237.

Noyes, E., Phillips, P. J. et O'Toole, A. J. (2017). What is a super-recogniser ? Dans *Face processing : Systems, disorders and cultural differences* (p. 173-201). Nova Science Publishers Inc.

O'Neil, C. (2016). *Weapons of math destruction*. New York, NY : Random House.

Pasquale, F. (2015). *The black box society*. Cambridge, MA : Harvard University Press.

Peng, Y. (2019). *Face recognition at a distance : Low-resolution and alignment problems* (Thèse de doctorat inédite). University of Twente.

Perruche, F. (2019, 18 septembre). Lyon : la reconnaissance faciale utilisée lors d'un procès suscite le débat. *RTL*. Repéré à https://www.rtl.fr/actu/justice-faits-divers/lyon-la-reconnaissance-faciale-utilisee-lors-d-un-proces-suscite-le-debat-7798350513

Phillips, P. J., Yates, A. N., Hu, Y., Hahn, C. A., Noyes, E., Jackson, K.,… O'Toole, A. J. (2018). Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms. *Proceedings of the National Academy of Sciences*, *115*(24), 6171-6176. https://doi.org/10.1073/pnas.1721355115

Rainie, L. et Duggan, M. (2016). *Privacy and information sharing* (p. 47). Washington, DC : Pew Research Center.

Ribaux, O. (2014). *Police scientifique : Le renseignement par la trace.* Lausanne, Suisse : Presses polytechniques et Universitaires Romandes.

Robertson, B., Vignaux, G. A. et Berger, C. E. H. (2016). *Interpreting evidence – Evaluating forensic science in the courtroom* (2e éd.). Chichester, Royaume-Uni : John Wiley & Sons, Ltd.

Rodriguez, A. M., Geradts, Z. et Worring, M. (2018). Validation of score-based likelihood ratio estimation for automated face recognition. *Northern Ireland*, 10.

Rossy, Q., Ioset, S., Dessimoz, D. et Ribaux, O. (2013). Integrating forensic information in a crime intelligence database. *Forensic Science International*, *230*(1), 137-146. https://doi.org/10.1016/j.forsciint.2012.10.010

Salas, R. (2020, 24 mars). Covid-19 – Les reconnaissances faciales chinoises et russes : entre protection sanitaire et surveillance de pointe. *Influencia*. Repéré à http://www.influencia.net/fr/actualites/tendance,pas-manquer,covid-19-reconnaissances-faciales-chinoises-russes-entre-protection-sanitaire-surveillance-pointe,10021.html

Sandberg, D. (2018). Face Recognition using Tensorflow. Github. Repéré à https://github.com/davidsandberg/facenet

SITA. (2017). *The passenger IT trends survey.* Montréal, Québec : Air Transport Industry Insights.

Smith, S. M., Stinson, V. et Patry, M. W. (2011). Fact or fiction ? The myth and reality of the CSI effect. *Court Review, 100*(47), 4-7.

Tistarelli, M. et Champod, C. (2017). *Handbook of biometrics for forensic science.* Cham, Suisse : Springer International Publishing AG.

Towler, A., Kemp, R. I., Burton, A. M., Dunn, J. D., Wayne, T., Moreton, R. et White, D. (2019). Do professional facial image comparison training courses work ? *PLOS ONE*, *14*(2), e0211037. https://doi.org/10.1371/journal.pone.0211037

Unisys Australia. (2014). *Unisys Security Index Report Australia – Biometrics in Airports.* Sydney, Australie.

Wang, M., Deng, W., Hu, J., Tao, X. et Huang, Y. (2019). Racial faces in-the-wild : Reducing racial bias by information maximization adaptation network. *arXiv : 1812.00194 [cs]*. http://arxiv.org/abs/1812.00194

Welsh, B. C. et Farrington, D. P. (2009). Public area CCTV and crime prevention : An updated systematic review and meta-analysis. *Justice Quarterly, 26*(4), 716-745. https://doi.org/10.1080/07418820802506206

Woodward, J. D. (2001). *Super Bowl surveillance : Facing up to biometrics.* RAND Corporation. Repéré à https://www.rand.org/pubs/issue_papers/IP209.html

Jurisprudence

Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993). United States Supreme Court.

R v. Mohan, 2 SCR 9 (1994). Supreme Court of Canada.

R v. Turner, 1 QB 834 (1975). Court of Appeal, UK.

Textes de loi

Code de procédure pénale (France). (1958). Repéré à https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071154

Code de procédure pénale suisse. (2007). Pub. L. No. RS 312.0. Repéré à https://www.admin.ch/opc/fr/classified-compilation/20052319/index.html

Federal Rules of Evidence. (2019). *Rule 702 – Testimony by Expert Witnesses.* U.S. Government publishing office.

Challenges and perspectives to face recognition in criminal science

ABSTRACT • *This article reviews practical challenges to and perspectives on the use of face recognition in criminal science. A better understanding of the limitations and opportunities of this technology is essential to determining how it should be used in the judicial system. We suggest that this reflection must be part of an interdisciplinary approach that integrates the use of algorithms while taking into account the unique characteristics of both criminology and forensic science. Determining the state of the art in the use of face recognition requires answering several fundamental questions. What sort of images are used in face recognition ? How are they compared ? What objectives does face recognition serve ? Where is it implemented and by whom ? These questions – and their answers – allow us to identify the challenges and shortcomings of face recognition, as well as perspectives on its development and research. At the data level, the main issue concerns the quality of the original image and its potential degradation during collection and storage, which can influence its subsequent use. At the methodological level, the stakes involve the lack of standardisation and transparency in tasks carried out by both humans and automatic systems. When looking at face recognition as used in the civil and judicial domains, questions arise around how to protect privacy and individual liberties. Finally, the main challenges raised by its use as evidence in court concern communication, as well as standardisation and methodological validation.*

KEYWORDS • *Face recognition, image, policing, forensic science, evidence.*

Desafíos y perspectivas del reconocimiento facial en las ciencias penales

RESUMEN • *El objetivo de este artículo es cristalizar de forma pragmática los desafíos y perspectivas del reconocimiento facial en las ciencias penales para adquirir un mejor conocimiento de los límites y oportunidades ofrecidos por estas tecnologías, que son esenciales para su aplicación en el sistema judicial. Postulamos que esta reflexión debe inscribirse dentro de una aproximación interdisciplinaria que integre el uso de algoritmos, considerando las especificidades de la criminología y de la ciencia forense. Este esclarecimiento permite establecer un estado del arte sobre el uso del reconocimiento facial, recortándolo en preguntas fundamentales: ¿Cuáles son las imágenes utilizadas para el reconocimiento facial? ¿Cómo son comparadas? ¿Cuáles son los objetivos del reconocimiento facial? ¿En dónde ha sido puesto en marcha y por qué actores? Esta subdivisión permite situar mejor los desafíos y los límites del reconocimiento facial, así como las perspectivas de desarrollo y de investigación. En lo que tiene que ver con los datos en sí, el desafío principal concierne su calidad original y su degradación potencial en las etapas de colecta y salvado de las imágenes que influencian su posterior uso. En lo que tiene que ver con los métodos, los desafíos se cristalizan alrededor de la falta de estandarización y de transparencia, tanto como en el momento de las funciones ejecutadas por el humano, como por un sistema automático. En lo que concierne a los objetivos de las funciones de reconocimiento facial en los campos civil y judicial, los desafíos gravitan alrededor de la protección de la esfera privada y de las libertades individuales. Finalmente, los desafíos principales subrayados por su uso como medio de prueba en el tribunal conciernen la comunicación así como la estandarización y la validación metodológica.*

PALABRAS CLAVE • *Reconocimiento facial, imagen, acción de seguridad, ciencia forense, elemento de prueba.*