

La vidéosurveillance algorithmique

Un état de surveillance est-il notre avenir ?

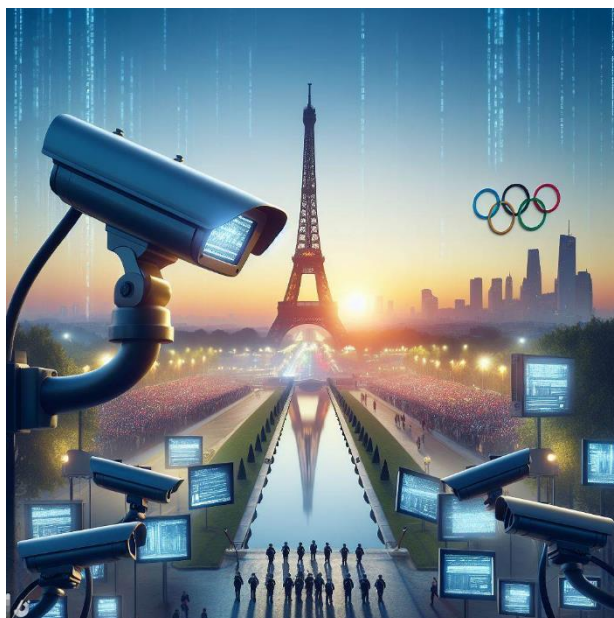


Illustration générée par Bing Image Creator

Ishfaq Rumjaun
Florent Pollet
Pierre-Louis Binachon
Aldair Olaya

Emilie Duval
Florestan Fontaine
Victor Pachy

2024

Cette publication a été réalisée par des étudiants en troisième année du cycle ingénieur de Mines Paris PSL Research University. Il présente le travail réalisé dans le cours intitulé « Descriptions de controverse », qui a pour objectif d'introduire les étudiants à l'univers incertain de la recherche scientifique et technique et de les sensibiliser aux enjeux de la participation citoyenne.

Mines Paris décline toute responsabilité pour les erreurs et les imprécisions que peut contenir cet article. Vos réactions et commentaires sont bienvenus. Pour signaler une erreur, réagir à un contenu ou demander une modification, merci d'écrire à la responsable de l'enseignement : madeleine.akrich@mines-paristech.fr.

Introduction

En novembre 2022, Randal Reid se rend en Géorgie avec sa mère pour le repas de Thanksgiving. Sur le trajet, il est arrêté par la police car il serait le principal suspect d'une affaire de vol de carte bleue en Louisiane qui a eu lieu quelques mois auparavant : il a été reconnu automatiquement par un logiciel de reconnaissance faciale intégré dans une caméra de vidéosurveillance. Le problème : Randal n'a jamais été en Louisiane de sa vie, et il n'a rien à voir avec le véritable suspect recherché par les forces de l'ordre. Les policiers n'ont même pas vérifié la taille et le poids de Randal qui ne correspondaient pas du tout à ceux du suspect initial, et ont fait preuve d'une confiance aveugle en la technologie de reconnaissance faciale. De ce fait, Randal Reid a passé une semaine en prison à tort.

La reconnaissance faciale est en théorie interdite en France aujourd'hui, mais les technologies de vidéosurveillance intelligente commencent même à se développer dans l'hexagone, comme le montre la loi relative aux Jeux Olympiques et Paralympiques de 2024 (appelée loi JO) qui a été votée le 19 mai 2023.

Dans l'article 10 de cette loi JO, il est stipulé que « les images collectées au moyen de systèmes de vidéoprotection autorisés [...] ou au moyen de caméras installées sur des aéronefs autorisés [...] dans les lieux accueillant ces manifestations et à leurs abords ainsi que dans les véhicules et les emprises de transport public et sur les voies les desservant, peuvent faire l'objet de traitements algorithmiques ».

Cette loi a pour but d'assurer la sécurité des événements propices à des « risques d'atteintes graves à la sécurité des personnes » à cause de l'ampleur de leur fréquentation notamment. Le traitement algorithmique permet de faciliter le travail des agents de sécurité en analysant automatiquement les images collectées dans le cadre légal. Même si cette loi a officiellement été votée dans le cadre de l'organisation des Jeux en 2024, sa portée temporelle (elle prévoit une autorisation d'un traitement algorithmique des images jusqu'à fin mars 2025) et sa formulation assez générale laissent croire à une utilisation plus importante de ce procédé.

Cette technologie porte un nom : la vidéosurveillance algorithmique. Elle permet, à l'aide d'un programme informatique, d'analyser de manière autonome une grande quantité d'images qu'il aurait été impossible de traiter – ou du moins aussi rapidement - de manière manuelle par un agent de sécurité. Pour cela, le programme informatique a été préalablement codé et entraîné à une tâche bien précise, qui peut aller de la détection de départ de feu, jusqu'à l'identification de personnes en passant par la détection de mouvements de foule importants.

Les programmes utilisés sont souvent dotés d'intelligence artificielle pour analyser les images. Il est donc naturel que la démocratisation de cette dernière ait permis à la vidéosurveillance algorithmique de connaître un essor considérable durant ces dernières années. En effet, la technologie semble prometteuse : par sa capacité à analyser une quantité importante d'images très rapidement, elle permettrait de détecter ce qui était longtemps resté invisible à l'œil faillible d'un agent de sécurité qui doit rester attentif à des dizaines d'écrans à la fois. Elle peut par exemple, attirer son attention sur une situation suspecte qui nécessiterait une surveillance particulière, ou lancer une alerte prévenant d'un événement possiblement dangereux en train de se produire.

Comme le témoigne ce projet de loi adopté l'année dernière, les pouvoirs publics semblent maintenant convaincus de l'apport de cette technologie en termes de sécurité nationale, et n'hésitent pas à investir des sommes importantes pour développer des réseaux de caméras équipées de vidéosurveillance algorithmique. Avec cette demande grandissante, de nombreuses start-ups françaises et internationales profitent de l'occasion pour proposer leurs offres. Parmi elles, Briefcam, une entreprise israélienne, possède désormais la majorité des parts de marché, et a déjà opéré des réseaux de caméras lors d'expérimentations dans plusieurs endroits en France comme Nice ou l'aéroport de Roissy-Charles-de-Gaulle. Les entreprises se livrent donc à une course

contre-la-montre pour récupérer un maximum de contrats, et cherchent à développer le meilleur logiciel de vidéosurveillance algorithmique.

Ce phénomène est très clairement visible dans la Figure 1, qui montre l'évolution du nombre de publications scientifiques traitant de la vidéosurveillance depuis 1980. On y voit une forte augmentation symptomatique de la volonté d'innover afin d'être à la pointe de cette technologie récente.

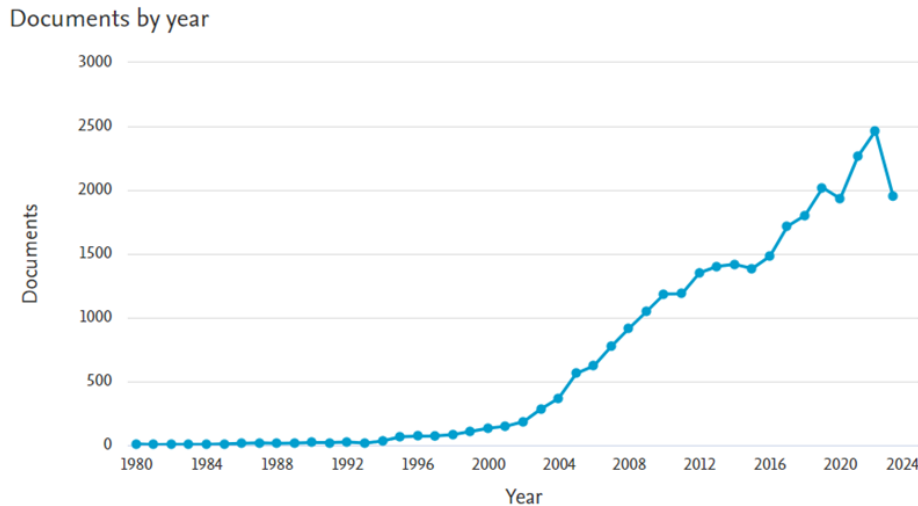


Figure 1 : Evolution du nombre de publications scientifiques traitant de la vidéosurveillance de 1980 à 2024

Plus que l'aspect commercial de la vidéosurveillance algorithmique, les citoyens eux-mêmes commencent à prendre conscience et à s'informer sur l'utilisation de cette technologie. Même si cela reste marginal pour le moment – peu de personnes ont conscience des expérimentations déjà réalisées par l'Etat dans plusieurs villes en France – la réglementation mise en place permet déjà de s'informer : l'article 10 de la loi citée plus haut impose aussi à la ville de Paris de prévenir les citoyens de la présence de caméras équipées de la vidéosurveillance algorithmique. Cependant, il est fort peu probable que la signalétique soit suffisante pour que les citoyens comprennent tous les enjeux qu'il y a derrière le développement d'une telle technologie...

On constate tout de même qu'une menace pèse sur les épaules des citoyens, la menace d'une société de surveillance, une société où la moindre erreur sera scrutée et analysée par les algorithmes, et où personne ne passera inaperçu. Une société où un citoyen pourra se faire arrêter sur la seule base du résultat d'un algorithme, sans aucun contrôle humain en entrée ou en sortie de celui-ci. Les citoyens semblent tout de même avoir conscience de cette menace, même si pour l'instant ils ne la connaissent que dans les livres qui décrivent le monde dystopique où tout le monde serait scruté sans arrêt par des robots, une atteinte forte aux libertés fondamentales. Un autre problème, plus insidieux, serait celui de la démultiplication des biais humains lorsqu'ils passent par le filtre d'un code informatique, avec le développement d'un algorithme qui aurait plus tendance à viser une certaine couleur de peau, une certaine zone géographique...

Cette dystopie aujourd'hui semble loin de notre société actuelle, mais peut-être que ces craintes sont fondées ? Arrivera-t-on à une normalisation de ces technologies de vidéosurveillance algorithmique, couplées à de la reconnaissance faciale ? Est-ce que les entreprises arriveront à convaincre les gouvernements de l'efficacité de leurs algorithmes pour pouvoir les installer partout ? Gagne-t-on en sécurité de ce que l'on donne de notre liberté en utilisant cette technologie ? N'allons-nous pas observer une croissance de la discrimination déjà présente aujourd'hui à cause de l'utilisation d'algorithmes qui ne laissent aucune place au doute et au jugement humain, plus mesuré ?

Beaucoup de questions auxquelles nous allons essayer de donner des éléments de réponse au cours de cet article, que nous allons segmenter en trois parties. Premièrement, nous nous poserons la question de si cette technologie apporte réellement une nouvelle couche d'efficacité aux technologies de vidéosurveillance existantes, puis nous analyserons la transparence de ces algorithmes, en nous demandant si elle sera suffisante pour éviter de potentiels biais discriminatoires. Enfin, nous verrons la place de la loi, et son potentiel rôle de garde-fou contre les dérives des technologies de vidéosurveillance algorithmique dans un monde où leur développement semble inévitable.

■ La VSA constitue-t-elle une nouvelle technologie de surveillance plus efficace que les dispositifs non automatisés ?

En termes de vocabulaire, il convient de distinguer la vidéoprotection qui est l'utilisation de caméras sur l'espace public, et la vidéosurveillance, qui elle se limite aux espaces privés. Dans la suite du développement, ces deux termes seront cependant utilisés indifféremment, puisque de nombreux acteurs utilisent à présent le terme vidéosurveillance pour des espaces publics également, non sans toutefois une connotation volontaire soulignant la potentielle intrusion dans la vie privée de ces nouvelles technologies.

■ De nouvelles fonctionnalités attendues par les opérateurs actuels

Sur la base du constat d'une croissance massive de la vidéoprotection en France depuis sa légalisation en 1995, le sociologue français Laurent Mucchielli estime à plus de 1.5 million¹ le nombre de caméras installées dans l'espace public, sous la responsabilité des mairies, à l'exception de Paris. Les flux vidéo sont visionnés et centralisés dans des centres de supervision urbaine (CSU), par des opérateurs, qui ont parfois plus de 50 écrans à superviser à la fois, ce qui est concrètement impossible à réaliser, comme le souligne le député de Vendée spécialisé sur les questions de données personnelles :

« il [l'agent] n'est pas capable d'avoir son attention portée sur chacun des écrans »

Par conséquent, deux pistes peuvent être envisagées pour tenter de remédier à cette situation : augmenter la main d'œuvre dans les centres urbains, qui n'est pas souhaitable économiquement ni socialement, ou développer de nouvelles solutions techniques pour aider le traitement en temps réel des flux des caméras.

C'est donc cette opportunité d'un nouveau marché avec un fort potentiel de croissance, en France comme à l'international, qu'ont saisi de nombreuses startups françaises et étrangères, que l'on peut retrouver à différents salons pros dont celui de l'événement mondial de la sûreté et la sécurité intérieure des Etats Milipol. Par exemple, l'entreprise israélienne BriefCam, appartenant à Canon, propose une solution complète qui intègre un module d'analyse en temps réel et d'alertes lorsque certaines situations définies à l'avance sont détectées. La société lilloise Neuronalys, quant à elle, développe une plateforme Neurocop, vendue avec un serveur dédié, qui est compatible avec n'importe quelle caméra actuelle et qui permet techniquement de réaliser un traitement en temps réel des données. Ces entreprises tiennent à souligner que leurs produits sont déjà matures car ils sont actuellement utilisés a posteriori pour faciliter la recherche lors d'enquêtes policières, et promettent donc un gain significatif d'efficacité en apportant davantage de sécurité par la détection de tous les événements potentiels dangereux. Par ailleurs, à l'étranger, des systèmes beaucoup plus perfectionnés sont employés, comme le *Domaine Awareness System* à New-York City. Thalès et Idemia développent également des solutions dans ce domaine.

Dans tous les cas, la vidéosurveillance algorithmique n'est censée consister qu'en un traitement en temps réel pour signaler aux opérateurs les situations considérées comme les plus dangereuses. Il ne s'agit en rien de prendre des décisions automatiquement et cela n'inclut pas d'utiliser des algorithmes mettant en jeu des informations de biométrie, selon la définition de la CNIL, qui sera rappelée par la suite. Même si beaucoup de solutions dans ce domaine existent déjà, et qu'elles sont très attendues par les opérateurs actuels, le court délai de préparation entre l'adoption de la loi JO permettant leur emploi et le déroulement des JO s'avère être un défi

¹ Le Devin W., Halissat I. (2018, 23, Mars) Laurent Mucchielli « La vidéosurveillance conduit souvent à un simple déplacement de la délinquance », Libération, Disponible sur https://www.liberation.fr/france/2018/03/23/laurent-mucchielli-la-videosurveillance-conduit-souvent-a-un-simple-deplacement-de-la-delinquance_1638345/

technique et logistique, pour adapter les solutions au cadre juridique défini. Le député de Vendée souligne effectivement que :

« ils [les députés] ont été traumatisés par la décision du conseil constitutionnel sur les drones et sur les caméras au moment de la loi sécurité globale. On a voté le texte beaucoup trop tard on aurait dû voter un an avant, passer les appels d'offre en fin 2022 / début 2023 pour être en captation d'image pendant 2023 pour préparer 2024 »

The screenshot shows the Neurocop interface. At the top, there is a grid of 15 location boxes. The first row contains: CROISEMENT DE CITE SUD 2, CROISEMENT RUE DE LA REPUBLIQUE, PEILLON DIRECTION ARTMAN, PEILLON DIRECTION MACON, PEILLON DIRECTION PLOMIE (with a red 'X' icon), PEILLON MAT, PEILLON ST-GEORGES, SORTIE A6, and SORTIE RUE DE LA REPUBLIQUE. The second row contains: ST GEORGES PEILLON, GRANDE RUE, ROND POINT CAVALIER 2, ROND POINT CAVALIER, ROUTE DE NEUVILLE BILEMONT, ROUTE DE NEUVILLE BILEMONT 2, RUE TRIEZ CAILLOUX ROUTE DE NEUVILLE, and VPI ROND POINT RUE DE LA LYS. Below the grid is a section titled 'Critères' with the instruction 'Indiquez sur quoi porte la recherche.' It includes six categories: Voitures, Véhicules lourds, 2 roues, Personnes (selected with a blue dot), Visages, and Animaux. Below this is a section titled 'Période' with the instruction 'Définissez la période de recherche.' It has two date and time pickers: 'Du : 01/01/2021 07:00' and 'Au : 06/10/2021 07:00'. At the bottom, there is a search bar labeled 'Nommer la recherche' with the text 'Pe' entered.

Figure 1: capture d'écran de l'interface de Neurocop

■ Un manque d'indicateurs précis sur l'efficacité actuelle et future des technologies

Si les industriels garantissent une efficacité décuplée grâce au traitement algorithmique des données, cette affirmation est remise en cause par des associations de défense des droits des libertés comme la Quadrature du Net. D'une part, celles-ci affirment l'inefficacité des caméras actuelles :

« Les partisans de la surveillance font ce constat qu'on se retrouve avec des tonnes et des tonnes de gigas de captation des espaces publics, qui n'ont aucune efficacité »

D'autre part, elles mettent en garde contre les promesses de la vidéosurveillance algorithmique. Elle ajoute :

« Avec ce constat d'échec de la technologie [de la vidéosurveillance], les volontés politiques veulent rajouter une autre couche de technologie pour essayer de la rendre efficace »

Ainsi, afin d'éviter d'investir dans des solutions qui ne sont potentiellement ni efficaces, ni désirables, il convient d'examiner de plus près les indicateurs sur l'efficacité des caméras de vidéosurveillance actuellement déployées. En effet, la Quadrature du Net ou encore Amnesty International mettent en garde contre le technosolutionnisme, selon lequel les techniques finiront par résoudre n'importe quel problème et constituent

donc la solution ultime à toutes les difficultés. Pour ces organismes, le recours abusif à cette idéologie conduit à une déresponsabilisation politique et à une neutralisation des critiques en coupant la réflexion car la technique s'appuie sur la science et elle ne serait donc pas discutable. Dans tous les cas, si l'efficacité de la VSA n'est pas nécessairement pratique, elle peut l'être du moins politiquement, pour garantir un sentiment de sécurité accrue pendant une période de menace terroriste élevée ou d'événements exceptionnels. En effet, certains argumentaires dénoncés par la Quadrature du Net comme « la VSA, elle aurait empêché le fiasco du stade de France » peuvent paraître convaincants pour une large majorité.

Des études scientifiques sur l'efficacité des caméras permettraient sûrement de proposer des données quantitatives pour pouvoir clore cette question ; toutefois, il en manque cruellement. A ce jour, il n'y a pas eu d'initiative commune ni approfondie entre les acteurs. Certes, la Cour des Comptes a publié en 2020 un rapport² sur les polices municipales, dans lequel elle critique la vidéosurveillance, notamment sur son efficacité pour la prévention de la délinquance et sur l'absence de statistiques fiables en France. Par ailleurs, quelques chercheurs comme Guillaume Gormand ont proposé des statistiques, ou certains ont choisi de se pencher sur les études faites à l'étranger. Ces dernières ont montré par exemple une baisse d'environ 70% du vol de véhicules dans les parkings³. Mais ces excellents résultats de prévention se limitent à des environnements clos et clairement définis, ce qui n'inclut pas la rue. L'étude de Guillaume Gormand a, quant à elle, conclu que cela n'aidait pas à l'élucidation de crimes. Toutefois, comme le rappelle le député de Vendée :

« Selon cette étude, les caméras ne servent à rien parce qu'elles n'ont pas permis d'identifier les personnes et d'aller faire la condamnation. Sauf qu'en pratique quand on regarde l'image c'est assez simple : on sélectionne une image où la personne coupable est visible, on l'envoie dans le TAJ [Traitement d'antécédents judiciaires] et on identifie éventuellement la personne. Si l'on identifie la personne, on va prendre sa téléphonie pour éventuellement aller faire une perquisition ; on va le convoquer ou aller l'arrêter et on va le mettre en garde à vue, on va le faire craquer, et il va parler à l'arrivée. Ce qui est retenu dans les procès-verbaux, ce n'est pas qu'on a eu l'image du coupable par la caméra, c'est qu'on l'a identifié et que la téléphonie a montré qu'il était sur place à ce moment-là. »

L'association Amnesty-International s'appuie également beaucoup sur cet argument pour demander une étude approfondie avant toute évolution technologique de la VSA :

« On n'a jamais prouvé qu'elles étaient efficaces pour lutter contre la criminalité ou autre. On n'a jamais fait d'études. C'est la Cour des Comptes qui le réclame depuis des années et on n'a aucune donnée scientifique objective qui montre une quelconque corrélation entre l'utilisation de la vidéosurveillance et, par exemple, le taux d'élucidation des crimes. Pour autant, on va en mettre plus. Si ça continue l'insécurité, on va rajouter une couche algorithmique par-dessus. On est dans une espèce de surenchère technologique, où, à chaque fois, si ça ne marche pas, ou si on n'a pas des résultats probants, il faut aller encore plus loin, on n'a pas fait assez. »

Bien qu'il y ait des débats sur l'efficacité de la vidéosurveillance algorithmique, elle continue d'être expérimenté et utilisé. Cela suscite des inquiétudes quant à l'utilisation de données sensibles et, en particulier, à l'atteinte à la vie privée.

² (2020, 20, Octobre), Les polices municipales, Cour des comptes, Disponible sur <https://www.ccomptes.fr/fr/publications/les-polices-municipales>

³ Le Goff T. (2010). Le faux et coûteux miracle de la vidéosurveillance, Après-Demain. Disponible sur <https://www.cairn.info/revue-apres-demain-2010-4-page-28.htm>

■ L'usage des données biométriques : le passage vers des données sensibles ?

Pour étudier la controverse liée à l'utilisation de données sensibles par les algorithmes de vidéosurveillance et à l'atteinte potentielle à la vie privée, il est tout d'abord nécessaire de définir clairement ce que sont les données capturées et traitées par l'algorithme.

Les données utilisées dans tous les algorithmes qui utilisent des informations personnelles pour identifier des individus, y compris les VSA, sont appelées données biométriques. Selon la définition officielle de la CNIL⁴:

« Les données biométriques sont des données personnelles car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales, etc.). »

La biométrie est un concept assez large, et lorsque nous limitons la discussion aux algorithmes de vidéosurveillance, les objets auxquels elle se réfère peuvent être des données sur le visage, l'apparence physique ou les caractéristiques comportementales d'une personne. De manière plus rigoureuse, le type de données biométriques utilisées par la VSA dépend de la conception de l'algorithme. En raison des différences entre les législations internationales relatives à la vidéosurveillance, différents algorithmes de vidéosurveillance capturent des informations personnelles avec des degrés de confidentialité variables. Par exemple, aux États-Unis, en Chine et à Singapour, le gouvernement autorise l'utilisation de la technologie de reconnaissance faciale dans les algorithmes de vidéosurveillance publique pour identifier les informations personnelles des citoyens (pas exclusivement à des fins de lutte contre la criminalité).

En revanche, en Europe, le Parlement européen a voté en juin 2023 l'interdiction totale de la reconnaissance faciale en temps réel dans les lieux publics. Et surtout, avec l'arrivée de la loi JO, les acteurs qui utilisent ces technologies développées affirment que la reconnaissance faciale n'est pas utilisée. Selon une directrice d'Ile de France Mobilités :

« La crainte d'être suivi, tracé et que l'on va tout savoir de moi relève du fantasme. La loi n'autorise toujours pas l'utilisation de la reconnaissance faciale, donc on oublie cette inquiétude-là. C'est une loi [Loi JO] qui autorise l'expérimentation sur des technologies très avancées. »

Toutefois, lors du Milipol Paris 2023, événement national de la sûreté et sécurité, une avocate au barreau de Paris affirme que :

« La reconnaissance faciale à ce jour, c'est prohibé mais pas à 100%. On a une marche de manœuvre qu'on essaie de respecter et mettre en place. »

En effet, la reconnaissance faciale en France est utilisée pour des aspects précis d'authentification comme le traitement des antécédents judiciaires (TAJ) et le système de passage rapide aux frontières extérieures (Parafe)⁵. Dans ces cas précis, les données collectées sont strictement encadrées dans des bases de données précises. Cependant, depuis la loi JO, quelques expérimentations ont été mises en place en France, notamment lors du carnaval de Nice en 2019 (vidéosurveillance placée sur un des portiques d'accès et environ 5000 personnes ont accepté de fournir une photographie de leur visage créant une nouvelle base de données). Des

⁴ Biométrie. CNIL Disponible sur <https://www.cnil.fr/fr/definition/biometrie>

⁵La Rédaction. (2023, 02, Novembre). Six questions sur la reconnaissance faciale. Vie Publique. Disponible sur [https://www.vie-publique.fr/questions-reponses/271221-six-questions-sur-la-reconnaissance-faciale#:~:text=En%20France%2C%20les%20dispositifs%20de,aux%20fronti%C3%A8res%20ext%C3%A9rieures%20\(Parafe\)](https://www.vie-publique.fr/questions-reponses/271221-six-questions-sur-la-reconnaissance-faciale#:~:text=En%20France%2C%20les%20dispositifs%20de,aux%20fronti%C3%A8res%20ext%C3%A9rieures%20(Parafe))

scénarios comme la recherche d'enfants perdus dans la foule ou la reconnaissance de personnes volontaires ont été testés. Pour le maire de Nice, les résultats sont très satisfaisants. Mais pour la CNIL, le rapport de l'expérimentation reste très vague notamment sur les questions techniques⁶.

Le principal problème, c'est qu'il n'y a pas de cadre juridique précis concernant les nouvelles technologies et notamment la reconnaissance faciale. Les expérimentations ont révélé la nécessité de renforcer le cadre juridique, ou bien comme le dit l'avocate au barreau de Paris :

« On doit mettre à l'épreuve la loi, qu'on ose définir un cadre légal fixe et qu'on le mette à l'épreuve, de la même manière que l'on teste les nouvelles technologies »

Pour l'instant, il existe un flou juridique complexifiant le caractère légal de l'utilisation de la vidéosurveillance algorithmique et la reconnaissance faciale, favorisant des potentielles dérives. En effet, les forces de l'ordre qui utilisent le logiciel « Vidéo Synopsis » de l'entreprise Briefcam pour traquer une personne sur un réseau de caméras peuvent facilement avoir accès à l'option de reconnaissance faciale inclus dans le logiciel. Selon Briefcam lors du Miliop 2023 :

« L'option de reconnaissance faciale est incluse dans le logiciel, les utilisateurs peuvent l'activer ou non »

De plus, beaucoup de recherches essayent d'intégrer les métadonnées et d'autres sources de données aux vidéosurveillances. C'est-à-dire, de permettre le croisement des données des réseaux sociaux ou localisations avec les données de vidéosurveillances afin de les enrichir. Ces innovations sur le croisement entraînent des préoccupations importantes sur les données sensibles.

Si toutes ces techniques de reconnaissance faciale et de croisement restent toutefois largement prohibées et peu utilisées, l'analyse des mouvements de foule est couramment utilisée et soulève aussi des préoccupations. Par exemple, pour Two-I, une start-up française basée à Metz conçoit ce que l'on appelle dans l'industrie des "plates-formes d'hyper-vision". Ces plateformes cartographient et transforment les masses de données collectées par les caméras et les algorithmes. Pour sécuriser les événements à forte affluence, la configuration unique de Mobil Security de BEHM est conçue pour surveiller 1 500 personnes par heure avec quatre agents. En intégrant la solution d'analyse vidéo Two-I (qui détecte à l'avance les bagages, les personnes à mobilité réduite et les personnes/véhicules non autorisés, etc.) ou encore son algorithme proposé lors de la pandémie de Covid-19, on est capable de détecter les personnes portant des masques et la température corporelle.⁷

L'algorithme de vidéosurveillance n'est pas basé sur le principe des données faciales mais plutôt sur l'identification et la surveillance d'individus anormaux dans la foule générale. Et comme le dit une juriste à La Quadrature du Net :

« Quand on sait où est quelqu'un à un moment à un endroit, elle n'est plus anonyme et sa vie privée est atteinte. »

Ainsi, que ce soit avec la reconnaissance faciale ou avec la détection de mouvement ou d'apparence, l'utilisation des données biométriques entraîne des préoccupations importantes sur les questions de collecte non

⁶Untersinger M. (2019, 28, août). Reconnaissance faciale : la CNIL tique sur le bilan de l'expérience niçoise. Le Monde. Disponible sur https://www.lemonde.fr/pixels/article/2019/08/28/reconnaissance-faciale-la-cnil-tique-sur-le-bilan-de-l-experience-nicoise_5503769_4408996.html

⁷ Two-I. Disponible sur <https://technopolice.fr/two-i/>

consensuelle d'informations personnelles et sur l'atteinte à la vie privée. Surtout le peu de détail technique existant pour expliciter l'algorithme peut entraîner des potentielles dérives comme la stigmatisation de groupe particuliers.

■ Transparence et contrôle humain : des mesures suffisantes contre les potentiels biais ?

La vidéosurveillance algorithmique est une technologie relativement récente sur laquelle nous manquons, comme nous l'avons vu plus tôt, d'indicateurs précis. Ce manque de clarté pour le grand public et les décideurs publics va au-delà de la question de l'efficacité et de nombreux acteurs s'interrogent sur l'objectivité réelle de ces algorithmes et sur la nécessité de mettre en place des mesures de contrôle.

La vidéosurveillance est déjà vue par certains acteurs du débat public comme une technologie de répression; la VSA se retrouve donc thématiquement associée à la disparition des libertés fondamentales et à la discrimination et la stigmatisation d'une partie de la population. La délégation de l'analyse à des programmes au fonctionnement obscur pour une grande majorité de la population n'a pas pour effet de rassurer sur l'absence de biais, bien au contraire. On peut observer un parallèle entre la montée du débat sur la VSA et le débat sur le caractère discriminatoire de la vidéosurveillance. La Figure 4 met en évidence une évolution similaire de l'importance accordée par les médias à la question de la VSA et à la question des discriminations liées à l'utilisation de la vidéosurveillance. En effet, cette perte de contrôle au profit de l'automatisation est un important vecteur de l'inquiétude liée à la vidéosurveillance comme moyen de stigmatisation des populations.

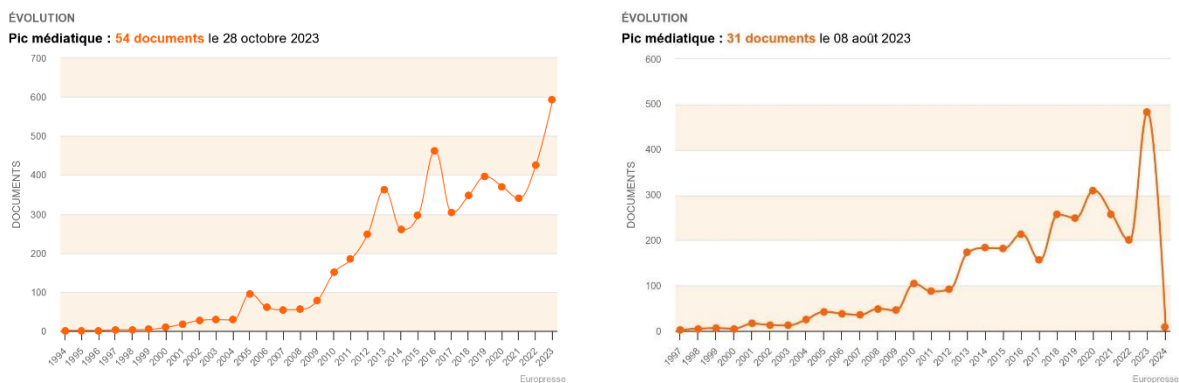


Figure 4 : évolution du nombre d'articles faisant référence à la VSA (à gauche) et du nombre d'article faisant référence à des conséquences discriminatoires à la vidéosurveillance (à droite) en France (Europresse)

Le législateur intéressé par les capacités de cette nouvelle technologie et l'industriel de la vidéosurveillance sont conscients de ces inquiétudes. Pour y pallier, ils promettent de mettre en place des processus de contrôle humain à même de lutter contre l'apparition de ces biais. Cependant, il est reproché aux industriels d'arrêter la transparence là où elle met en danger leurs intérêts économiques et les garanties mises en place, notamment dans l'article 10 de la loi JO, ne font, pour ainsi dire, pas tout à fait l'unanimité. Néanmoins, le Conseil Constitutionnel, à la suite d'une saisine par des députés, conclura, sous certaines réserves, à la conformité de l'article avec le respect des libertés fondamentales.

- **Les risques liés à l'existence de biais automatisés : des vecteurs potentiels de discriminations ?**

L'une des premières questions posées quand on traite des biais dont pourraient faire preuve la VSA est l'étendue de son application, ou plus précisément les événements ou comportements qu'elle va définir comme anormaux. A ce sujet, l'article 10 de la loi JO⁸ définit et limite le cadre d'application de la VSA à "l'indication du ou des événements prédéterminés qu'ils ont été programmés à détecter", les événements en question devant être liés à des "risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes". Les dispositions de cette loi ont été critiquées par plus de 60 députés qui ont alors procédé à la saisine du conseil constitutionnel. Ces députés ont notamment reproché à ces dispositions de méconnaître la liberté d'aller et de venir, le droit de manifester, la liberté d'opinion ainsi que le droit au respect de la vie privée. De nombreuses associations se sont également opposées à cette loi pour des raisons similaires. Par exemple, dans une lettre ouverte, 38 associations européennes⁹ publient l'avis suivant sur la loi JO :

« Nous estimons que les mesures de surveillance introduites sont contraires au droit international relatif aux droits humains dans la mesure où elles ne satisfont pas aux principes de nécessité et de proportionnalité et impliquent des risques inacceptables vis-à-vis de plusieurs droits fondamentaux tels que le droit à la vie privée, le droit à la liberté de réunion et d'association et le droit à la non-discrimination. Si l'article était adopté, il créerait un précédent inquiétant en matière de surveillance injustifiée et disproportionnée dans l'espace public, au détriment des droits fondamentaux et des libertés. »

En plus de menacer les libertés fondamentales de la population dans son ensemble, pour des associations comme La Quadrature du Net¹⁰, les propositions faites dans la loi JO sont loin de garantir la neutralité de ces outils. Au contraire, cette association estime que cette loi amènera la mise en place d'outils à caractère discriminatoires. Elle considère que l'élaboration des algorithmes ne constitue pas une pratique neutre, détachée du monde social, car à l'inverse, l'interprétation des images par logiciel reproduit les mêmes biais qu'avaient ceux qui l'ont programmée. Ainsi, en fonction de ce que les personnes à l'origine des programmes définissent comme un comportement anormal, cela mènera à des discriminations. Un des exemples donnés est la détection automatique du « maraudage » (le fait d'être statique dans l'espace public), permettant d'automatiser l'action de la police, et que l'association dénonce comme « une chasse aux personnes mendiant », sous couvert de la protection de l'espace public.

Un autre facteur régulièrement décrié par les acteurs opposés à la VSA, comme étant facteur de biais et discriminations pour ces outils, est le choix de bases données sur lesquelles sont entraînés ces outils, et qui influenceraient également ce que les algorithmes vont considérer comme suspect. C'est un point soulevé entre autres par la CNIL¹¹, qui considère également les algorithmes comme porteurs de choix normatifs derrière leur apparente neutralité. Elle ajoute également que ces biais pourraient avoir un impact important sur les personnes. Un exemple donné par plusieurs acteurs est l'utilisation des outils de la VSA aux Etats-Unis. La surreprésentation de personnes noires dans les images fournies pendant l'entraînement de l'algorithme conduit l'algorithme à considérer de manière inhérentes la population noire comme plus suspecte, donc plus à risque d'être discriminé.

⁸ Journal officiel "Lois et Décrets" (JORF n° 0116 du 20 mai 2023). Disponible sur <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047561974/> [Consulté le 23/10/2023]

⁹ European Center for Not-for-Profit Law (2023, 06, mars). Civil society public letter on the proposed French law on the 2024 Olympic and Paralympic Games. Disponible sur <https://ecnl.org/news/civil-society-open-letter-proposed-french-law-2024-olympic-and-paralympic-games#:~:text=The%20proposal%20would%20lead%20to,pretext%20of%20securing%20big%20events>. [Consulté le 28/12/2023]

¹⁰ La Quadrature du Net (2023, 5, janvier). Mobilisation générale contre la légalisation de la vidéosurveillance automatisée !. Disponible sur <https://www.laquadrature.net/2023/01/05/mobilisation-generale-contre-la-legalisation-de-la-videosurveillance-automatisee/>. [Consulté le 10/11/2023]

¹¹ CNIL (2022). CAMÉRAS DITES « INTELLIGENTES » OU « AUGMENTÉES » DANS LES ESPACES PUBLICS. Disponible sur <https://www.cnil.fr/fr/cameras-dites-augmentees-dans-les-espaces-publics-la-position-de-la-cnil>. [Consulté le 24/11/2023]

Au-delà de ces potentiels vecteurs de biais et discriminations qui peuvent apparaître comme fortuits, les opposants à la VSA critiquent certains aspects discriminatoires purement intentionnels, et avoir des conséquences concrètes sur la population. Un membre de La Quadrature du Net dénonce ainsi les logiciels vendus par Briefcam qui auraient des capacités de filtrage en fonction du genre, de la couleur de peau, des vêtements... Ce type de filtres est considéré par la plupart des opposants comme discriminatoire par leur simple existence, car ils permettraient de différencier le traitement de différentes catégories de population. Mais ce membre de La Quadrature du Net ne doute pas que ces possibilités seront utilisées à mauvais escient, voire abusées par les forces de l'ordre dont, selon la personne interrogée, les pratiques racistes ont été largement documentées. Même en l'absence de ce type de filtres, il faudrait toujours craindre les abus des possibilités qu'ils offrent.

L'utilisation de la VSA pour la stigmatisation de certains groupes spécifiques pourrait porter atteinte à leurs droits à la vie privée et de réunion. En plus des biais présents, en surface ou en caché sous les algorithmes, dans ces nouveaux outils, ces derniers présentent les mêmes risques de discrimination que la vidéosurveillance classique. Ainsi favoriser l'implantation des caméras dans certains quartiers plutôt que d'autres est également vecteur de stigmatisation de catégories de populations pour Amnesty International¹². Placer dix fois plus de caméras dans les quartiers pauvres conduirait à la surreprésentation des interventions policières dans ces quartiers. La présence policière plus importante conduirait alors à une plus forte répression qui pourrait mener à une modification subie des comportements, voire une privation de libertés.

Les technologies de Machine Learning utilisées pour la VSA pourraient même conduire à l'amplification de ces biais plutôt qu'à leur atténuation. Ainsi, pour un membre d'Amnesty International, les biais donnés en entrée à l'algorithme vont être décuplés et amplifiés par la puissance informatique, et les conséquences seront pires qu'avec la simple action humaine. La personne interviewée a alors donné en exemple une étude sur les technologies de reconnaissance faciale utilisées par les forces de l'ordre à New York, qui aurait conclu qu'elles avaient tendance à amplifier les pratiques de maintien de l'ordre discriminatoires et racistes. D'une certaine manière, ces algorithmes pourraient échapper au contrôle de leur créateur dans la mesure où ils peuvent même encoder des biais inconscients. Le créateur ne se rend pas lui-même compte du caractère discriminatoire, et donc problématique de son nouvel outil.

■ Vers un processus de contrôle humain en amont et en aval de la VSA ?

La solution principalement avancée par les promoteurs de la VSA et réclamée par les autorités de contrôle pour pallier les éventuels biais présents dans les algorithmes est un processus de contrôle continu et suivi. La CNIL juge nécessaire la mise en place systématique d'un contrôle humain pour signaler les biais qui apparaissent pendant l'utilisation de ces algorithmes¹³. En effet, elle juge nécessaire de :

« garantir les principes de vigilance (visant à se prémunir de la tentation de délégation à ces outils) et de loyauté (afin de s'assurer que l'utilisation des outils correspond à celle attendue) »

¹² Amnesty International (2022). Facial recognition threatens fundamental rights when it works, and also when it doesn't work. Disponible sur <https://banthescan.amnesty.org/nyc/>. [Consulté le 14/01/2024]

¹³ CNIL (2022). CAMÉRAS DITES « INTELLIGENTES » OU « AUGMENTÉES » DANS LES ESPACES PUBLICS. Disponible sur <https://www.cnil.fr/fr/cameras-dites-augmentees-dans-les-espaces-publics-la-position-de-la-cnil>. [Consulté le 24/11/2023]

La principale solution proposée pour garantir la protection de ces principes est la mise en place d'organismes spécialisés dans le contrôle de ces technologies pour une surveillance systématique de leur utilisation.

Ce contrôle nécessite donc d'avoir un minimum de retour sur les résultats fournis par les algorithmes. Le Conseil Constitutionnel¹⁴ estime par ailleurs qu'il est de la responsabilité du législateur de ne mettre en place que des traitements algorithmiques permettant de :

« vérifier l'objectivité des critères retenus et la nature des données traitées ainsi que comporter des mesures de contrôle humain et un système de gestion des risques de nature à prévenir et à corriger la survenue de biais éventuels ou de mauvaises utilisations »

Il faut comprendre par-là que le législateur a la charge de mettre en place tous les outils de contrôle nécessaire à chaque événement où il est décidé de recourir à la VSA pour éviter des situations où surviennent, voire simplement où pourraient survenir, les biais décrits plus tôt. A la suite de sa saisine par les 60 députés, le conseil constitutionnel a conclu à la conformité de l'article 10 de la loi JO à ce principe :

« Ainsi, le législateur a veillé à ce que le développement, la mise en œuvre et les éventuelles évolutions des traitements algorithmiques demeurent en permanence sous le contrôle et la maîtrise de personnes humaines. Compte tenu de ces différentes garanties [...], le Conseil constitutionnel juge que les dispositions contestées ne méconnaissent donc pas le droit au respect de la vie privée. »

Il apparaît en tout cas clairement que, pour les promoteurs de la VSA, l'objectif immédiat n'est pas la délégation totale du pouvoir de décision aux algorithmes. La majorité des projets décrits par les entreprises de la vidéosurveillance décrivent ces outils comme de simples outils de traitement de données permettant de faire remonter aux opérateurs les informations les plus importantes. Aucune action n'est effectuée par l'algorithme, et il revient toujours à un humain de décider de la réaction à ces informations et de déterminer si elles soulèvent une quelconque nécessité d'intervention de la part des forces de l'ordre.

Le deuxième point soulevé régulièrement par les autorités de contrôle est la nécessité de transparence avec le public. Cela se traduirait notamment par la mise en place de moyens de communication en amont des événements où la VSA est mise en place, pour prévenir du cadre et de l'étendue de l'utilisation de ces technologies. Le Conseil Constitutionnel a, par exemple jugé nécessaire que le public soit « préalablement informé, par tout moyen approprié, de l'emploi de traitements algorithmiques sur les images collectées »¹⁵. Il a néanmoins émis une réserve en cas de circonstances particulières interdisant cette communication ou en cas de contradiction avec les objectifs poursuivis.

Il apparaît néanmoins évident qu'en l'état actuel de cette technologie, seule une minorité extrême du public est compétente pour évaluer sérieusement la présence de ces biais. Pour la CNIL¹⁶ :

¹⁴ Conseil Constitutionnel (2023, 17, mai). Décision n° 2023-850 DC du 17 mai 2023. Disponible sur <https://www.conseil-constitutionnel.fr/decision/2023/2023850DC.htm>. [Consulté le 14/12/2023]

¹⁵ Conseil Constitutionnel (2023, 17, mai). Décision n° 2023-850 DC du 17 mai 2023. Disponible sur <https://www.conseil-constitutionnel.fr/decision/2023/2023850DC.htm>. [Consulté le 14/12/2023]

¹⁶ CNIL (2022). CAMÉRAS DITES « INTELLIGENTES » OU « AUGMENTÉES » DANS LES ESPACES PUBLICS. Disponible sur <https://www.cnil.fr/fr/cameras-dites-augmentees-dans-les-espaces-publics-la-position-de-la-cnil>. [Consulté le 24/11/2023]

« si les citoyens peuvent constater et, d'une certaine manière, appréhender l'installation de différentes caméras vidéo dans leur quotidien, ils n'ont pas de moyen d'avoir conscience que celles-ci peuvent également les analyser, ni de quelle manière et sur quels critères cette analyse fonctionne »

Car en réalité seule une partie infime de la population comprend concrètement comment fonctionne ce genre de technologies, et serait alors à même de les juger. Ces technologies sont particulièrement difficiles à évaluer car les logiciels fonctionnent par des méthodes d'apprentissage automatique de type Deep Learning, des boîtes noires qui ne sont réellement maîtrisées que par une poignée d'experts. D'autant que ces programmes, par leur nature même, sont difficilement interprétables, et on ne peut comprendre leur raisonnement. Ce potentiel manque de compréhension des enjeux semble en tout s'être traduit par un manque d'investissement du grand public sur cette thématique, les acteurs, que nos analyses ont relevés, étant en grande majorité rapport direct avec le droit, la protection des libertés fondamentales ou la vidéosurveillance elle-même. Les acteurs s'étant particulièrement investis sont mêmes s'une certaine façon surreprésentés dans le débat public de la VSA.

Pour le président d'un think tank interrogé, ce manque de compréhension du fonctionnement de ces outils est également présent chez le législateur qui ne comprend pas forcément ce qu'implique la mise en place d'une telle technologie. Il rejoint également un député interrogé dans la mesure où il comprend l'objectif qu'ont actuellement les entreprises de vidéosurveillance à garder leurs modèles fermés, c'est-à-dire empêcher les personnes extérieures à l'entreprise de se rendre compte du fonctionnement interne de l'algorithme ; la technologie est inaccessible. Cette propension à ne distribuer ni le code de leurs outils, ni les données sur lesquelles ils ont été entraînés s'explique simplement car il y a un intérêt commercial majeur à garder le monopole de production de ces outils, et qu'il faut éviter de donner aux concurrents les clés pour copier leur projet. La transparence totale demandée au législateur va alors à l'encontre du secret industriel nécessaire aux entreprises.

Face aux acteurs s'inquiétant des potentielles dérives discriminatoires de la VSA, il appartient au législateur, comme l'a confirmé le Conseil Constitutionnel, de mettre en place des processus de contrôle humain pour lutter contre les biais et de mettre en place les moyens de communications nécessaires pour informer, voire éduquer le public à ces technologies. Pour mettre en place ces outils censés protéger les concitoyens, le législateur est désormais amené à endosser la responsabilité morale de protéger les libertés fondamentales que sont la liberté d'aller et venir, la liberté d'association et le droit à la vie privée. Cependant ce rôle, et donc ce pouvoir accordé au législateur, et par le législateur, soulève de nouvelles inquiétudes.

■ De l'expérimentation technoscientifique à la normalisation sociopolitique : quelles garanties juridiques pour assurer les droits fondamentaux et les libertés individuelles ?

L'avènement de la loi JO a marqué une étape significative dans la réglementation des systèmes de vidéosurveillance automatisée et soulève des questions sur la normalisation de ces technologies dans la société. Cette législation a ouvert la voie à des expérimentations suscitant à la fois intérêt et préoccupation quant à leurs répercussions à long terme.

Cependant, la loi JO n'est pas le seul terrain d'expérimentation concrète de ces dispositifs. Plusieurs acteurs, tels qu'Amnesty International¹⁷, La Quadrature du Net¹⁸ ou encore Disclose¹⁹, affirment que des expérimentations ont été menées sur le terrain alors que la VSA était interdite, dépassant ainsi que le caractère scientifique, hors de tout cadre légal, de l'expérimentation de nouvelles technologies. La place de la loi dans le développement de l'innovation est alors sujet à controverse. Le contexte législatif, axé sur la régulation des VSA, a donné lieu à des débats intenses sur les implications sociétales et éthiques de ces expérimentations et a suscité des inquiétudes quant à l'équilibre délicat entre la sécurité publique et les droits individuels à la vie privée. Si certains voient dans ces expérimentations une opportunité de mieux appréhender ces technologies émergentes, d'autres insistent sur la nécessité de poser dès maintenant les fondations d'un cadre réglementaire approprié en définissant des limites claires et en garantissant des mécanismes de contrôle robustes²⁰.

Il est considéré par certains acteurs tels que le député Renaissance de Vendée (un des dépositaires de la proposition de loi JO) ou le directeur d'un laboratoire d'idées sur l'économie numérique, comme essentiel de comprendre et maîtriser ces nouvelles technologies dans un monde où leur développement semble inévitable. Plutôt que de faire face à des problèmes dus à une mise en œuvre tardive et à des difficultés de compréhension, il serait préférable de chercher à comprendre et à réguler leur intégration dès maintenant. A cet argument, d'autres - tels que La Quadrature du Net ou Amnesty International - répondent en remettant en question cette inévitabilité. En effet, une inquiétude majeure porte sur la possibilité de voir émerger une société de surveillance où la collecte et l'analyse à grande échelle de données pourraient compromettre les libertés individuelles. Les expérimentations permises par la loi JO pourraient ainsi remodeler les normes de surveillance en introduisant de nouvelles pratiques pouvant affecter la sphère privée des citoyens et influencer sur le fonctionnement démocratique dans la chronologie de mise en place de lois. En ouvrant la voie à d'autres dispositifs de surveillance accrue, ces technologies pourraient exercer une influence croissante sur la sphère privée des individus, sans même que ceux-ci ne mesurent les risques qu'ils encourent, notamment car cette arrivée progressive des technologies toujours plus robustes entraîne une forme « d'accoutumance des individus à la surveillance », notamment des jeunes qui « n'ont connu que ça », comme le soulève le directeur du think tank mentionné précédemment. Il est à craindre que cette tendance ne conduise à une société dans laquelle « la sécurité est plus importante que la protection des droits », une évolution dénoncée par Amnesty International, justifiant ainsi le déploiement de toujours plus de technologies, via des processus qui pourraient manquer d'encadrement législatif et ne respectent pas nécessairement les procédures. L'analyse se concentre alors ici sur les implications des expérimentations, législatives ou non, dans le domaine de la surveillance automatisée. Il est notamment essentiel d'évaluer comment

¹⁷ (2023, 20, Mars). Les technologies intrusives de surveillance lors des Jeux olympiques pourraient inaugurer un avenir dystopique. Amnesty. Disponible sur URL [Consulté le 09/01/2024]

¹⁸ (2023, 05, Avril). Vidéosurveillance biométrique : Derrière l'adoption du texte, la victoire d'un lobby. La Quadrature du Net. Disponible sur URL [Consulté le 09/01/2024]

¹⁹ (2023, 14, Novembre). La Police nationale utilise illégalement un logiciel israélien de reconnaissance faciale. Disclose. Disponible sur URL [Consulté le 09/01/2023]

²⁰ Denis. (2023, 06, Juillet). Des actions juridiques contre la vidéosurveillance. Halte au contrôle numérique. Disponible sur URL [Consulté le 09/01/2023]

ces expérimentations pourraient non seulement influencer le paysage de la surveillance mais également remodeler les rapports entre l'État, les entreprises et les citoyens dans le contexte numérique actuel.



Figure 5 : Parade et campagne pour la candidature de Paris aux Jeux Olympiques 2024

■ Innover dans les nouvelles technologies pour mieux prévenir d'éventuelles dérives

Selon le député de Vendée :

« le futur est aux IA et la surveillance, la sécurité et la protection n'y échapperont pas, d'autant plus que ce sont des technologies très en vogue en Chine ou au Japon par exemple mais également dans des pays occidentaux comme aux Etats-Unis et en Europe ».

Les technologies d'IA génératives connaissant un grand essor ces dernières années, le questionnement de leur utilisation dans de nombreux sujets s'est posé.

Cependant, l'utilisation d'IA pour la sécurité et la surveillance n'est pas nouvelle. L'État Chinois a commencé à utiliser la VSA dès 2008 pour les JO de Pékin, Londres a fait de même en 2012. De même, la reconnaissance faciale est de plus en plus commune dans les établissements privés comme les bâtiments d'entreprise privilégiant la reconnaissance faciale pour éviter les badges.

Documents by country or territory

Compare the document counts for up to 15 countries/territories.

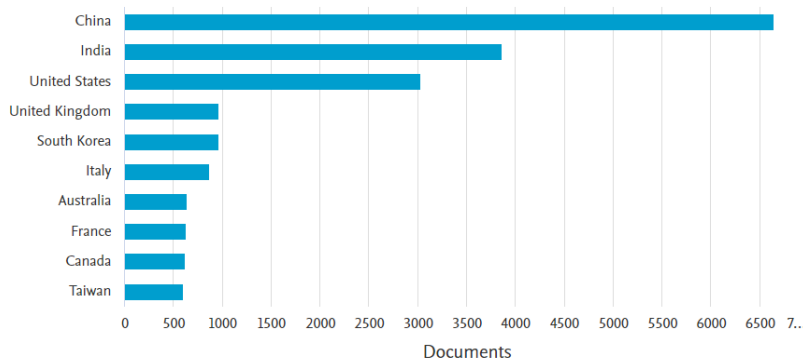


Figure 6 : évolution du nombre d'articles faisant référence à la Vidéosurveillance par pays d'origine dans Scopus entre 2010 et 2024

La Figure 6 met en évidence la considération importante de certains pays asiatiques pour la vidéosurveillance et à fortiori de la vidéosurveillance algorithmique dans des pays comme la Chine, l'Inde ou les Etats-Unis. La tendance mondiale sur ce sujet est à la hausse et principalement portée par des géants asiatiques ou nord-américains.

On peut alors supposer qu'il n'y aura pas de contingence quant à l'utilisation générale de l'IA dans les systèmes de protection ou d'utilisation privée. Entre la Chine et les Etats-Unis dont les investissements en IA n'ont cessé d'augmenter ces 10 dernières années²¹, l'Europe se trouve entre deux géants et devra décider entre interdire totalement l'utilisation d'IA dans la vidéosurveillance et dénoter du reste du monde ou alors suivre le flux général.

Dans les deux scénarios, l'IA sera tellement présente dans la sécurité privée en France et qu'elle offrira tellement de praticité et elle inondera inévitablement la sécurité publique d'ici une vingtaine d'années. Les deux scénarios se résument alors selon lui à accepter l'IA dès maintenant et grandir avec afin de maîtriser ses écarts et réguler en réaction son utilisation en France, ou dans un second temps laisser la conjoncture mondiale décider à notre place et subir son existence dans deux décennies. Être pionnier dans l'industrie de l'intelligence artificielle et de l'IA peut être une condition nécessaire pour atteindre une souveraineté nationale ou européenne, sans subir l'influence des politiques nord-américaines ou chinoises. L'Europe doit tirer ses propres leçons de l'utilisation de l'IA et se forger son propre avis, ses propres législations.

Il y a une volonté forte de l'Europe « d'être pionnière sur les sujets de régulation et d'encadrement » selon un représentant d'un think tank sur les questions de progrès numérique. Cependant, être l'arbitre des élégances et des technologies ne suffit pas à gagner le match, il faut en être aussi l'acteur. Milipol Paris, le salon des acteurs de sûreté et de sécurité intérieure des États, regroupe un très grand nombre d'industriels du domaine défendant tous la même idée : la législation freine le développement technologique et économique de ces entreprises. Or, selon Laurent Pellegrin, directeur France de l'entité sécurité publique et identité d>IDEMIA et invité de la table ronde à Milipol Paris 2023, les industriels doivent être le « fer de lance de l'IA pour la sécurité », plutôt que de subir une législation trop restrictive.

²¹ (2021, 25, Janvier). Intelligence artificielle : l'Europe distancée par la Chine et les Etats-Unis. Capital. Disponible sur URL [Consulté le 09/01/2024]

■ La nécessaire expérimentation de la vidéosurveillance algorithmique

Cette volonté d'être pionnier mais surtout de ne pas prendre de retard dans l'utilisation de l'IA pour la sécurité et la sûreté, mais surtout dans la vidéosurveillance algorithmique, nécessite donc selon les sympathisants de cette technologie une démarche active dans l'utilisation. La loi JO pour 2024 intervient alors comme une première étape pour l'expérimentation d'une telle technologie en France.

Trois principales raisons sont avancées pour cette approche expérimentale. Tout d'abord, sur le plan technologique, il existait une incertitude quant à ce qui serait efficace. Contrairement à d'autres pays où des systèmes spécifiques, tels que des caméras 4K, ont été déployés, à Paris, les caméras de la mairie de Paris, de la SNCF et de la RATP ont été utilisées, avec une résolution parfois limitée, nécessitant des algorithmes adaptés.
22

Ensuite, une réticence sociale importante était ressentie, même si elle pouvait être justifiée par la nature exceptionnelle de l'événement. Ainsi, il était impératif d'encadrer strictement l'utilisation de l'algorithme dans le temps et dans l'espace, en se limitant à des cas spécifiques de situations normales. De plus, il était prévu de fixer une date de fin pour cette expérimentation afin de faciliter la gestion sociale complexe de cette technologie.²³

Enfin, la troisième raison résidait dans l'incertitude opérationnelle quant à la manière dont les forces de l'ordre utiliseraient l'algorithme pendant les JO. À cela s'ajoute le fait que l'IA ACT, un dispositif en cours d'élaboration, n'était pas encore finalisé au moment de la rédaction de la loi. Pour pallier ces incertitudes, un périmètre très restreint a été défini pour encadrer l'expérimentation, avec l'intention de procéder à une évaluation approfondie du système avant de décider de sa pérennité. Malgré ces précautions, des contraintes légales et une nécessité de trouver un équilibre entre sécurité et liberté ont été imposées par le Conseil Constitutionnel, laissant entrevoir la possibilité d'une réévaluation future du sujet.²⁴

Cependant, cette expérimentation pour les JO est fortement critiquée justement sur son caractère expérimental qui est remis en cause. Selon Amnesty International,

« si l'on avance au-delà de la ligne rouge une fois, cela sera trop tard pour revenir en arrière ».

Cette loi JO qui se présente initialement comme une solution aux risques liés aux JO est alors plutôt comme une première étape de la démocratisation de la vidéosurveillance algorithmique. Amnesty accuse cette expérimentation JO de ne réellement servir que d'acte d'existence de la VSA car les expérimentations existent déjà.

En effet, Disclose, un média d'investigation, a récemment publié une enquête révélant que depuis 2015, la France et la police nationale utilisaient un logiciel de VSA développé par l'entreprise israélienne BriefCam²⁵. Ce logiciel permet la reconnaissance sociale, une capacité qui n'est pas clairement encadrée par la loi. L'enquête

²² Panta F. J. (2020). Modélisation des métadonnées multi sources et hétérogènes pour le filtrage négatif et l'interrogation intelligente de grands volumes de données : application à la vidéosurveillance. Thèse de doctorat, Institut de Recherche en Informatique, Toulouse. Disponible sur URL [Consulté le 09/01/2023]

²³ Pouré. (2023, 20, Mars). JO de Paris 2024 : pourquoi la vidéosurveillance automatisée fait débat. Le Monde. Disponible sur URL [Consulté le 09/01/2023]

²⁴ (2021, 22, Septembre). Règlement IA : La commission européenne tend le piège de la reconnaissance faciale. La Quadrature du Net. Disponible sur URL [Consulté le 09/01/2023]

²⁵ (2023, 14, Novembre). La Police nationale utilise illégalement un logiciel israélien de reconnaissance faciale. Disclose. Disponible sur URL [Consulté le 09/01/2023]

met en lumière le fait que ces expérimentations se sont déroulées en dehors d'un cadre légal, car il n'existait pas de réglementation spécifique pour le développement de la VSA ou de la reconnaissance faciale. La loi JO est mentionnée comme étant récemment adoptée pour établir un premier cadre légal dans ce domaine. Cependant, les expérimentations illégales, révélées par les journalistes, ont été menées en secret pendant huit ans.

L'article indique que la police utilisait le logiciel sans avoir déclaré son utilisation à la Commission nationale de l'informatique et des libertés (CNIL), une obligation légale en France. Les journalistes ont obtenu des emails de cadres de la police reconnaissant qu'ils n'avaient pas respecté cette obligation, soulignant ainsi le caractère clandestin de ces opérations.

Selon Amnesty, ces expérimentations servent à normaliser l'utilisation de la VSA et de la reconnaissance sociale, préparant ainsi le terrain pour une utilisation plus large à l'avenir en France. La nouvelle loi JO est présentée comme une tentative de poser un cadre légal, mais le texte suggère que l'expérimentation en cours continuera, avec une évaluation prévue avant mars 2025 pour décider de sa reconduction. [10]

Depuis 2015, la France a manifesté une volonté claire d'élargir les pouvoirs de surveillance, en particulier ceux de la police, en utilisant des technologies de surveillance. Cette orientation s'est concrétisée avec la loi sur le renseignement et, plus récemment, avec la loi JO, l'ajout d'une couche algorithmique à la vidéosurveillance, y compris l'utilisation de drones.

On peut souligner une surenchère technologique avec des expérimentations, telles que la vidéosurveillance algorithmique, qui servent à normaliser ces technologies et à accroître leur acceptabilité sans remise en question. La loi JO, bien que temporaire et expérimentale, fait de la France le premier État membre de l'UE à légaliser la vidéosurveillance algorithmique, ce qui pourrait être reconduit compte tenu des raisons évoquées.

La dimension politique de cette décision s'inscrit dans un contexte plus large au sein de l'Union européenne, avec l'IA Act récemment adopté. Cette législation propose une approche par les risques, visant à identifier les technologies incompatibles avec les droits humains et à les interdire, établissant ainsi une hiérarchie de régulation en fonction des niveaux de risques. Le Parlement Européen a adopté une position jugée protectrice des droits humains, avec l'interdiction des technologies présentant un risque significatif.

■ Le rôle de la loi dans l'encadrement des progrès techniques

L'évolution constante des avancées technologiques pose un défi fondamental au cadre législatif établi. La place de la loi dans ce contexte de progrès techniques rapides et continus est au cœur de débats cruciaux. En effet, alors que les technologies évoluent à un rythme effréné, le processus législatif peine souvent à suivre, créant un écart significatif entre les développements technologiques et les cadres juridiques régulateurs. Cette situation soulève des questions majeures sur la capacité des réglementations actuelles à s'adapter aux innovations technologiques émergentes, ainsi que sur la pertinence et l'efficacité des lois existantes pour encadrer ces évolutions.

Dans ce contexte, explorer le rôle de la loi face au progrès technique revêt une importance cruciale pour garantir un équilibre entre l'innovation technologique, la protection des droits individuels et la préservation des principes démocratiques. Les délais dans l'établissement des réglementations ou dans l'adoption d'expérimentations sont souvent attribués, selon le député de Vendée, à un défi général : l'administration met du temps pour prendre des décisions en raison d'une méconnaissance voire d'une incompréhension des nouvelles technologies. Ce retard devient presque une norme, où la législation est constamment en décalage avec les avancées technologiques. Ainsi, dans la préface de Le droit au contact de l'innovation technologique, Henri Oberdoff estime qu'

« au contact de l'innovation technologique, le droit est défié, parfois sommé de réagir pour combler ce qui est [...] faussement décrit comme le « vide juridique » ».

Ce schéma n'est alors pas spécifique à la loi JO et se répète dans divers projets. Le député de Vendée souligne par exemple que l'administration a été fortement marquée par la décision du Conseil Constitutionnel concernant l'utilisation des drones et des caméras lors de l'élaboration de la loi sécurité globale. Cette expérience a créé une sorte de paralysie, entraînant un retard d'un an dans le vote du texte par rapport au calendrier initial. Cette situation a également impacté le déploiement des nouvelles technologies, retardant ainsi la calibration appropriée des dispositifs de contrôle prévus pour la Coupe du Monde de Rugby, notamment les scanners millimétriques, retardant ainsi leur mise en place effective.²⁶

Mais malgré la création de ces délais, la loi a ses raisons d'intervenir avant la mise en place d'une technologie de sécurité publique puisqu'elle vise à prévenir les abus potentiels, à encadrer l'utilisation de technologies émergentes et à établir des lignes directrices pour leur utilisation future. Elle a donc un effet de prévention et d'anticipation. De plus, la législation est conçue pour protéger les droits individuels et la vie privée, et pour garantir une utilisation éthique et équitable des technologies de sécurité publique. La loi établit ainsi des limites et des règles pour éviter les abus et assurer une utilisation conforme aux normes éthiques et légales, ce qui la rend nécessaire dans une société démocratique et peut expliquer les délais qu'elle implique : les enjeux de protection des citoyens sont de taille et il faut être certain que les mesures adoptées seront suffisantes et éviter des situations de vide juridique ou des situations où les réglementations ne s'appliquent pas adéquatement aux nouvelles réalités technologiques.

C'est alors dans ce cadre que des acteurs tels qu'Amnesty International mettent en garde contre les expérimentations non encadrées : de quelle garantie dispose-t-on quant à la protection – entre autres – des droits des citoyens ? Comme le rappelait le Conseil Constitutionnel lors d'un communiqué de presse sur la « Loi relative aux Jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions » du 17 mai 2023,

« La mise en œuvre de tels systèmes de surveillance doit être assortie de garanties particulières de nature à sauvegarder le droit au respect de la vie privée. ».

Cependant, les entreprises qui développent ces technologies peuvent naviguer à la lisière de la légalité, profitant du laps de temps entre l'émergence des avancées technologiques et l'établissement des réglementations. Cette

²⁶ (2023, 19, Janvier). Les Jeux de Paris terrain d'expérimentation de nouvelles méthodes sécuritaires. Le Monde. Disponible sur URL [Consulté le 09/01/2023]

fenêtre temporelle permet l'utilisation des technologies sans qu'elles soient pleinement encadrées par la loi. Ainsi, depuis 2017 la Commission Nationale de l'Informatique et des Libertés (CNIL) met en lumière la différence entre la vidéosurveillance traditionnelle et la vidéosurveillance algorithmique, soulignant que

« ces outils de vidéo protection ne sont en aucun cas une simple extension technique des caméras existantes »

mais différent tant par leurs modes de fonctionnement que par leurs objectifs et posent donc de « nouvelles questions éthiques et juridiques ». Cependant, comme cela a été mentionné précédemment, des entités telles que les municipalités ont exploité cette zone grise pour déployer ces dispositifs avant l'élaboration d'un cadre réglementaire approprié, et ce, sans en informer les citoyens, ce qui questionne le caractère démocratique de ce déploiement qui navigue aux limites de la légalité.

En réalité, comme l'explique le directeur du think tank sur l'économie numérique, le message en France (comme en Allemagne et en Italie) est – bien que surprenant dans un pays attaché aux réglementations – d'« innover avant de réguler ». Par ailleurs, cette démarche expérimentale - quand bien même encadrée comme c'est le cas pour les JO – comporte des risques inhérents. Elle pourrait induire un précédent déterminant qui, une fois établi, pourrait s'imposer dans l'évolution future de la législation sur la surveillance et les technologies connexes. Ce caractère expérimental soulève des questions sur la manière dont ces essais seront conduits, sur l'interprétation de leurs résultats et sur l'influence de ces données d'essai sur les réglementations à venir. L'expérimentation n'est pas neutre, non pas seulement au sens où elle est un site de collaboration entre le public et le privé, mais aussi parce qu'elle constitue un moyen d'action de l'Etat pour contribuer à l'innovation. En effet, le caractère d'exception de la loi JO est discutable. D'une part, elle ne vaut pas seulement pour les JO mais aussi pour les manifestations sportives, culturelles et festives de grande ampleur. D'autre part, les expérimentations sont le plus souvent généralisées :

« Il est rare qu'un retour en arrière se produise, surtout après le déploiement d'un tel investissement financier »

d'après une chargée de plaidoyer pour Amnesty International. Le député de Vendée le reconnaît : l'une des raisons du recours à l'expérimentation est de « prévenir la réticence sociale » face à la création d'une nouvelle loi qui semble particulièrement intrusive. D'ailleurs, l'Histoire prouve – dans des situations similaires – que le déploiement de technologies sécuritaires via des expérimentations dans le cadre de manifestations sportives tend à perdurer : le déploiement de la reconnaissance faciale en Russie suite à la Coupe du monde de football en 2018 ainsi que la généralisation de la vidéosurveillance à Londres après les JO de 2012 en sont deux exemples. On pourrait dire qu'ici, c'est autant par l'expérimentation que par la régulation que l'Etat gouverne. Il semble alors légitime de se questionner si cette approche ne tend pas à devenir une pratique standard pour promouvoir l'adoption d'un projet de loi ou du moins instaurer de nouvelles pratiques de surveillance. Le directeur du think tank semble suggérer cette idée lorsqu'il explique :

« La réalité, c'est que si vous regardez l'actualité depuis 2001, le terrorisme est un bon prétexte pour faire beaucoup d'expérimentations et on est dans ce duel permanent depuis 20 ans maintenant au nom de la protection des libertés. »,

laissant entendre que la sécurité peut être utilisée comme justification de certaines dérogations à la loi.

■ Conclusion

La vidéosurveillance algorithmique (VSA) soulève des questions complexes et controversées, notamment en France où la vidéoprotection a connu une croissance exponentielle depuis sa légalisation en 1995. L'émergence de technologies automatisées offre des opportunités pour pallier les limitations actuelles. Cependant, la mise en œuvre de ces solutions soulève à la fois des défis logistiques et juridiques.

L'efficacité de la vidéosurveillance actuelle est sujette à débat, avec des opinions divergentes entre les industriels et les défenseurs des droits individuels. Les données sur l'efficacité réelle des caméras de vidéosurveillance sont - aujourd'hui - insuffisantes, laissant place à des revendications contradictoires. La Quadrature du Net met en garde contre le technosolutionnisme, soulignant la nécessité d'une évaluation objective plutôt que d'une surenchère technologique.

Un aspect particulièrement sensible est l'utilisation de données biométriques dans la VSA, relevant potentiellement de données sensibles. La définition des données biométriques par la CNIL souligne leur caractère unique et permanent. Bien que des différences législatives existent à l'échelle internationale, les préoccupations en matière de vie privée sont universelles, comme en témoigne l'interdiction de la reconnaissance faciale en temps réel dans les lieux publics votée par le Parlement européen en 2023. En outre, le flou juridique actuel renforce la nécessité d'un cadre légal précis pour encadrer ces technologies, minimisant ainsi les risques de dérives potentielles. En l'absence de données scientifiques objectives, la prudence et la vigilance sont nécessaires pour garantir une utilisation responsable et éthique de la VSA.

La VSA suscite des inquiétudes croissantes quant à ses potentiels biais et à leur impact sur les libertés fondamentales. Le manque de clarté entourant cette technologie, en particulier son objectivité réelle, produit des préoccupations quant à la transparence des algorithmes et à la nécessité de mesures de contrôle.

Associée thématiquement à la disparition des libertés fondamentales et à la stigmatisation de certaines populations, la VSA est critiquée pour la délégation de l'analyse à des programmes dont le fonctionnement obscur accroît les inquiétudes sur les biais, comme par exemple, la discrimination liée à des biais automatisés, telle que la détection du "maraudage", sont soulevés. Cela nécessite de définir des critères objectifs et de protéger les droits individuels.

Les dispositions législatives actuelles, notamment l'article 10 de la loi JO, sont sujettes à controverse, critiquées pour leur potentiel impact sur la vie privée, le droit de manifester et la liberté d'opinion. Des associations européennes soulignent que de telles mesures peuvent être contraires au droit international relatif aux droits humains, mettant en danger des principes tels que la nécessité et la proportionnalité. Face à ces préoccupations, les promoteurs de la VSA proposent la mise en place de processus de contrôle humain en amont et en aval de l'utilisation de cette technologie. La CNIL souligne l'importance d'un contrôle continu pour garantir la vigilance et la loyauté, tandis que le législateur est appelé à assurer la transparence et à informer le public sur l'utilisation de ces technologies.

Cependant, la complexité des algorithmes de la VSA rend difficile la compréhension pour la majorité du public, soulignant le besoin de moyens efficaces de communication. Le législateur doit ainsi endosser la responsabilité morale de protéger les libertés fondamentales tout en éduquant le public. Toutefois, la question du pouvoir accordé au législateur suscite de nouvelles inquiétudes quant à d'éventuels abus.

La promulgation de la loi JO a inauguré une étape cruciale dans la régulation des systèmes de VSA, provoquant des interrogations quant à la normalisation de ces technologies au sein de la société. Cette législation a ouvert la voie à des expérimentations suscitant des intérêts et des préoccupations quant à leurs répercussions à long terme. Cependant, l'expérimentation des dispositifs de VSA ne se limite pas au cadre de la loi JO, comme le soulignent plusieurs acteurs tels qu'Amnesty International, La Quadrature du Net, et Disclose. Des expérimentations ont été menées même lorsque la VSA était interdite, causant ainsi des débats intenses sur les

implications sociétales et éthiques mais aussi des préoccupations quant à son potentiel impact sur la vie privée et les droits individuels.

Certains estiment que ces expérimentations offrent une opportunité pour mieux comprendre ces technologies émergentes, tandis que d'autres insistent sur la nécessité d'établir un cadre réglementaire dès maintenant, définissant des limites claires et garantissant des mécanismes de contrôle robustes.

Les acteurs pro VSA considèrent essentiel de comprendre et de maîtriser ces nouvelles technologies dès maintenant, argumentant que l'avenir appartient aux intelligences artificielles et qu'il est donc crucial l'acceptation de l'IA pour maîtriser son développement et réguler son utilisation. La question se pose de savoir si l'Europe doit suivre l'exemple de la Chine et des États-Unis ou adopter une approche indépendante pour éviter une future dépendance.

L'évolution rapide des technologies pose un défi à la législation, qui peine souvent à suivre le rythme. Le rôle de la loi dans ce contexte est fondamental pour assurer un équilibre entre l'innovation technologique, la protection des droits individuels et la préservation des principes démocratiques. Cependant, les retards législatifs peuvent créer des fenêtres temporelles où les entreprises exploitent des avancées technologiques sans encadrement juridique complet.

Pour finir, le panorama complexe de la VSA révèle une dualité entre l'innovation technologique et la nécessité de protéger les droits individuels. Naviguant entre l'urgence de la sécurité et la prévention des abus potentiels, il devient impératif de créer un équilibre. L'avenir de la VSA nécessite une réflexion approfondie, une anticipation législative, et une participation active des acteurs tant publics que privés pour façonner une utilisation éthique et responsable de ces technologies émergentes. Face à ces défis, la société doit évoluer avec prévoyance, se gardant de sacrifier les fondements démocratiques au nom de la sécurité.

■ Matériel et méthodes

Le présent travail résulte tout d'abord d'une analyse de la presse nationale et internationale, du début des archives à nos jours, au sujet de la vidéosurveillance algorithmique, de son implantation législative et de points de controverses soulevés. La base de données Europresse a été consultée au moyen de cinq équations de recherches différentes : " vidéosurveillance & (augmentée | algorithmique | automatique | automatisée) ", " vidéosurveillance & (lobby | lobbys | lobbying | lobbyiste) ! (PSG | abattoirs | abattoir) ", " vidéosurveillance & JO ", " reconnaissance faciale " et " vidéosurveillance & (biais | discrimination | stigmatisation) ".

Les corpus de documents recueillis pour chaque équation ont fait l'objet de deux types d'analyse distincts : une analyse sémantique avec la plateforme CorText et un traitement statistique des données textuelles avec le logiciel IRaMuTeQ. Les regroupements de termes ont permis d'identifier de nouveaux acteurs de la controverse et de mettre en évidence les liens, ou le cas échéant leur absence, entre les différents nœuds de la controverse. L'étude bibliographique a été complétée par la lecture, l'analyse et le référencement d'articles scientifiques traitant d'algorithmes de vidéosurveillance automatique, et ce, grâce à la consultation de la base de données Scopus.

Ce travail a également été enrichi par des lectures des textes législatifs liés à la problématique, notamment la loi JO (LOI n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 [...]) et l'AI Act (Proposition de règlement du parlement européen et du conseil établissant des règles harmonisées concernant l'intelligence artificielle [...]), afin de mieux appréhender les tensions relatives à ces textes. Il a également été étudié la chronologie du processus législatif de ces lois, notamment la loi JO, qui au cœur de la montée en puissance de la controverse dans le débat public.

La première étape a consisté en un état des lieux qui a permis non seulement d'identifier les différentes positions sur ce sujet, mais aussi les institutions publiques et privées impliquées ainsi que les personnes les représentant.

La deuxième étape a nécessité d'entrer en contact avec les acteurs afin de pouvoir les interviewer et leur poser les questions nécessaires pour approfondir leur position institutionnelle et obtenir des détails sur les solutions qu'ils proposent. Les entretiens ont eu lieu en personne et par vidéoconférence en ligne, selon la disponibilité des personnes. Dans les deux cas, des notes ont été prises sur les réponses, et le contenu a été transcrit pour pouvoir les citer dans notre article. Nous avons eu l'occasion d'échanger avec :

- une chargée de plaidoyer d'une association internationale de défense des droits
- une juriste d'une association nationale de défense des droits numériques
- un député français, spécialisé les questions de données personnelles
- une juriste et un ingénieur IA du régulateur français des données personnelles
- un directeur d'un think-tank spécialisé sur les questions d'IA
- différents acteurs présents au salon Milipol

La troisième et dernière étape a consisté à structurer l'article en le nourrissant de l'analyse quantitative, des entretiens et de la lecture bibliographique. L'objectif était de traiter les nœuds de la controverse et d'essayer de présenter de la manière la plus neutre possible les différents points de vue, sans manifestation objective liée aux propres jugements de valeur des rédacteurs de l'étude.

Références

■ Articles de presse généraliste / presse professionnelle

Le Devin W., Halissat I. (2018, 23, Mars) Laurent Mucchielli « La vidéosurveillance conduit souvent à un simple déplacement de la délinquance », Libération, Disponible sur https://www.liberation.fr/france/2018/03/23/laurent-mucchielli-la-videosurveillance-conduit-souvent-a-un-simple-deplacement-de-la-delinquance_1638345/

(2020, 20, Octobre), Les polices municipales, Cour des comptes, Disponible sur <https://www.ccomptes.fr/fr/publications/les-polices-municipales>

Biométrie. CNIL Disponible sur <https://www.cnil.fr/fr/definition/biometrie>

La Rédaction. (2023, 02, Novembre). Six questions sur la reconnaissance faciale. Vie Publique. Disponible sur [https://www.vie-publique.fr/questions-reponses/271221-six-questions-sur-la-reconnaissance-faciale#:~:text=En%20France%2C%20les%20dispositifs%20de,aux%20fronti%C3%A8res%20ext%C3%A9rieures%20\(Par afe\)](https://www.vie-publique.fr/questions-reponses/271221-six-questions-sur-la-reconnaissance-faciale#:~:text=En%20France%2C%20les%20dispositifs%20de,aux%20fronti%C3%A8res%20ext%C3%A9rieures%20(Par afe))

Untersinger M. (2019, 28, août). Reconnaissance faciale : la CNIL tique sur le bilan de l'expérience nicoise. Le Monde. Disponible sur https://www.lemonde.fr/pixels/article/2019/08/28/reconnaissance-faciale-la-cnil-tique-sur-le-bilan-de-l-experience-nicoise_5503769_4408996.html

20 mars 2023. Les technologies intrusives de surveillance lors des Jeux olympiques pourraient inaugurer un avenir dystopique. Amnesty. Disponible sur URL [Consulté le 09/01/2024]

05 avril 2023. Vidéosurveillance biométrique : Derrière l'adoption du texte, la victoire d'un lobby. La Quadrature du Net. Disponible sur URL [Consulté le 09/01/2024]

14 novembre 2023. La Police nationale utilise illégalement un logiciel israélien de reconnaissance faciale. Disclose. Disponible sur URL [Consulté le 09/01/2023]

Denis. (2023, 06, Juillet). Des actions juridiques contre la vidéosurveillance. Halte au contrôle numérique. Disponible sur URL [Consulté le 09/01/2023]

25 janvier 2021. Intelligence artificielle : l'Europe distancée par la Chine et les Etats-Unis. Capital. Disponible sur URL [Consulté le 09/01/2024]

Pouré. (2023, 20, Mars). JO de Paris 2024 : pourquoi la vidéosurveillance automatisée fait débat. Le Monde. Disponible sur URL [Consulté le 09/01/2023]

(2021, 22, Septembre). Règlement IA : La commission européenne tend le piège de la reconnaissance faciale. La Quadrature du Net. Disponible sur URL [Consulté le 09/01/2023]

07 septembre 2023. Coupe du monde de rugby : dernier sursis avant l'avènement d'une société sous vidéosurveillance algorithmique ? Amnesty. Disponible sur URL [Consulté le 09/01/2023]

19 janvier 2023. Les Jeux de Paris terrain d'expérimentation de nouvelles méthodes sécuritaires. Le Monde. Disponible sur URL [Consulté le 09/01/2023]

European Center for Not-for-Profit Law (2023, 06, mars). Civil society public letter on the proposed French law on the 2024 Olympic and Paralympic Games. Disponible sur <https://ecnl.org/news/civil-society-open-letter-proposed-french-law-2024-olympic-and-paralympic-games#:~:text=The%20proposal%20would%20lead%20to,pretext%20of%20securing%20big%20events.> [Consulté le 28/12/2023]

La Quadrature du Net (2023, 5, janvier). Mobilisation générale contre la légalisation de la vidéosurveillance automatisée !. Disponible sur <https://www.laquadrature.net/2023/01/05/mobilisation-generale-contre-la-legalisation-de-la-videosurveillance-automatisee/>. [Consulté le 10/11/2023]

Amnesty International (2022). Facial recognition threatens fundamental rights when it works, and also when it doesn't work. Disponible sur <https://banthescan.amnesty.org/nyc/>. [Consulté le 14/01/2024]

▪ Thèse, mémoires

Panta F. J. (2020). Modélisation des métadonnées multi sources et hétérogènes pour le filtrage négatif et l'interrogation intelligente de grands volumes de données : application à la vidéosurveillance. Thèse de doctorat, Institut de Recherche en Informatique, Toulouse. Disponible sur URL [Consulté le 09/01/2023]

▪ Ouvrages

Le Goff T. (2010). Le faux et coûteux miracle de la vidéosurveillance, Après-Demain. Disponible sur <https://www.cairn.info/revue-apres-demain-2010-4-page-28.htm>

▪ Littérature grise

Two-I. Disponible sur <https://technopolice.fr/two-i/> [Consulté le 14/01/2023]

Journal officiel "Lois et Décrets" (JORF n° 0116 du 20 mai 2023). Disponible sur <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047561974/> [Consulté le 23/10/2023]

11 CNIL (2022). CAMÉRAS DITES « INTELLIGENTES » OU « AUGMENTÉES » DANS LES ESPACES PUBLICS. Disponible sur <https://www.cnil.fr/fr/cameras-dites-augmentees-dans-les-espaces-publics-la-position-de-la-cnil>. [Consulté le 24/11/2023]

Conseil Constitutionnel (2023, 17, mai). Décision n° 2023-850 DC du 17 mai 2023. Disponible sur <https://www.conseil-constitutionnel.fr/decision/2023/2023850DC.htm>. [Consulté le 14/12/2023]