



Master II

Droit et Stratégies de la Sécurité

L'EXPÉRIMENTATION DES CAMÉRAS « AUGMENTÉES » : Une évolution sécuritaire au mépris des libertés ?

Mémoire préparé sous la direction de
Madame Pascale MARTIN-BIDOU

Présenté et soutenu publiquement par
Arnaud DENEUVE

Année universitaire 2023-2024

**L'EXPÉRIMENTATION DES
CAMÉRAS « AUGMENTÉES » :**
Une évolution sécuritaire au mépris des libertés ?

REMERCIEMENTS

À Madame Pascale MARTIN-BIDOU pour son aide et sa disponibilité dans la réalisation de ce mémoire de recherche.

À mes co-directeurs de Master, Mme MARTIN-BIDOU et M. DEBOVE pour m'avoir permis d'intégrer ce parcours où les cours de Master 2 sont dispensés au sein de l'Ecole des Officiers de la Gendarmerie Nationale.

« L'Université n'entend donner aucune approbation ni improbation aux opinions émises dans le mémoire ; ces opinions doivent être considérées comme propres à leur auteur ».

TABLE DES ABRÉVIATIONS

CJA : Code de justice administrative

CE : Conseil d'Etat

Conv.EDH : Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales

C.Cass : Cour de cassation

Cour.EDH : Cour européenne des droits de l'homme

CJUE : Cour de Justice de l'Union européenne

CNIL : Commission nationale de l'informatique et des libertés

CSI : Code de la sécurité intérieure

Déclaration de 1789 : Déclaration des droits de l'homme et du citoyen

IA : Intelligence artificielle

JOP 24 : Jeux Olympiques et Paralympiques 2024

Loi JOP : Loi relative aux Jeux Olympiques et Paralympiques et portant autres diverses dispositions

LOPS 1995 : Loi d'Orientation et de Programmation de la Sécurité du 21 janvier 1995

RGPD : Règlement général sur la protection des données

SILT : Sécurité Intérieure et Lutte contre le Terrorisme (issus de la loi du 30 octobre 2017)

SOMMAIRE

TITRE I : LE RECOURS EXPÉRIMENTAL AUX CAMÉRAS « AUGMENTÉES » ET LE RENOUVELLEMENT DE LA QUESTION DE LA PROTECTION DE LA VIE PRIVÉE

- Chapitre 1 : Le cadre juridique de l'article 10 de la loi du 19 mai 2023 concernant le déploiement des caméras « augmentées »
- Chapitre 2 : Les nécessaires garanties de protection de la vie privée lors du recours aux caméras « augmentées »

TITRE II : LE RENFORCEMENT DU CONTRÔLE NON JURIDICTIONNEL DES SYSTÈMES DE VIDÉOPROTECTION ET L'ÉLABORATION D'UNE RÈGLEMENTATION RELATIVE À L'INTELLIGENCE ARTIFICIELLE

- Chapitre 1 : L'expérimentation des caméras « augmentées » mettant en valeur cette technologie et le rôle de la CNIL
- Chapitre 2 : Vers une réglementation de l'intelligence artificielle au niveau européen

INTRODUCTION GÉNÉRALE

*« Pas d'angle mort, d'où le surnom donné à Argos :
Panoptès – « celui qui voit partout » –, parce qu'il
est le meilleur surveillant de toute la Terre »¹.*

Argos Panoptès donna son nom au concept philosophique éponyme, le panoptique, développé par Jeremy BENTHAM au XVIII^e siècle. Ce concept, d'abord développé dans le cadre carcéral, consiste à voir sans être vu. Concrètement BENTHAM va appliquer ce concept à la prison dans le but de rendre utile les prisonniers en leur enlevant toute idée de faire du mal². Pour BENTHAM la finalité du panoptique est le processus de civilisation des prisonniers. Michel FOUCAULT va donner une autre dimension à ce concept en l'élargissant à l'ensemble de la société dans son ouvrage *Surveiller et punir*. En effet, pour FOUCAULT le panoptique pourrait conduire à moins punir que prévenir en ce que les citoyens exerceraient un contrôle social sur les autres et réprimeraient par la même occasion leurs actions violentes. Le panoptique est également un concept architectural pour pouvoir mettre en oeuvre son principe fondamental : « voir sans être vu ». « Avec l'avènement des nouvelles technologies, le panoptique quitte chaque jour davantage l'univers carcéral pour essaimer une colonie de surveillances au-delà des hauts murs de la prison »³. Les défenseurs des libertés voient dans ce concept ce que pourrait être n'importe quel État, c'est-à-dire un État de surveillance permanente des citoyens. Cela est décrit par George ORWELL dans sa célèbre dystopie *1984* avec le fameux *Big Brother is watching you*.

¹ « Argos est doté d'au moins deux paires d'yeux, devant et derrière – ou même, selon les sources, d'une centaine ou d'une infinité. La multiplicité de son regard fait que jamais ses multiples paupières ne se ferment en même temps. Pas d'angle mort, d'où le surnom donné à Argos : Panoptès – « celui qui voit partout » –, parce qu'il est le meilleur surveillant de toute la Terre. Au sens grec du verbe « voir », il incarne l'homme théorique, boule omnidirectionnelle d'yeux ouverts, et, en termes d'images, rien ne lui échappe ». Serres (M.), Écoutez voir – L'histoire d'Argos et Hermès dans Philosophie magazine, 2013 in La Boussole: <https://laboussole.coop/2021/01/05/recueil-de-citations-sur-les-themes-de-la-surveillance-et-de-lintime/> (consulté le 27 février 2024).

² Site de radio France: <https://www.radiofrance.fr/franceculture/le-panoptique-a-l-origine-de-la-societe-de-surveillance-8706244> (consulté le 04 mars 2024).

³ (F.) DEBOVE, « Surveiller et punir dans un monde 3.0 », *AJPénaL*, Dalloz, Chronique de déontologie de la sécurité n°3, n° 202203, mars 2022.

Toutes les technologies de surveillance mises en place par les gouvernements sont perçues par ceux qui les combattent comme des moyens de réduire les libertés des personnes sous couvert de vouloir mieux garantir leur sécurité. Néanmoins, dans notre société hyper-connectée, avec des *smart city*⁴ qui se développent partout dans le monde, chaque personne détient un moyen de surveillance des individus avec les caméras de leurs téléphones qu'ils utilisent en permanence. Cette situation est décrite par Robin RIVATON sous le concept de « sousveillance »⁵. Cet auteur décrit le paradoxe qui entoure la vidéo puisque d'un côté la surveillance d'origine étatique est combattue, alors que la vidéo qui provient des personnes et qui est souvent publiée sur les réseaux sociaux est très bien conservée et acceptée⁶.

Le développement des nouvelles technologies dans le domaine de la sécurité s'est accentué notamment depuis la période de la pandémie de COVID-19 pendant laquelle les forces de l'ordre avaient utilisé des drones pour surveiller le respect du confinement. Cela a été suspendu par le Conseil d'État le 18 mai 2020⁷, avant qu'un cadre juridique ne soit établi par la loi du 25 mai 2021⁸. Que ce soit pour faire respecter les règles sanitaires ou pour lutter contre les menaces comme le terrorisme, les autorités publiques ont de plus en plus besoin de recourir aux nouvelles technologies afin d'assurer la sécurité de la population et le maintien de l'ordre public, que Victor HUGO décrit comme « le calme extérieur »⁹. La menace terroriste reste toujours l'une des luttes prioritaires malgré la défaite militaire de l'État islamique depuis 2017. En effet, cette « séquence ouverte depuis 2012 ne s'est pas encore définitivement fermée »¹⁰. Selon la Direction Générale de la Sécurité Intérieure « depuis 2012, les attentats terroristes ont causé la mort de 273 personnes et fait de très

⁴ Définition de la *smart city* par la CNIL, <https://www.cnil.fr/fr/definition/smart-city>.

⁵ (R.) RIVATON, *Sourions, nous sommes filmés ! Pour un discours optimiste sur les caméras*, Paris, Éditions de l'Observatoire, coll. Alpha Essai, 2023, p. 14.

⁶ *Ibid*, p. 21.

⁷ CE, ord. référé, 18 mai 2020, n° 440442.

⁸ Loi, n° 2021-646, 25 mai 2021 *pour une sécurité globale préservant les libertés*.

⁹ (V.) HUGO, *Le dernier jour d'un condamné*, Classiques, édition Pocket, p. 36. « *Il s'était établi entre la foule et les charrettes je ne sais quel horrible dialogue ; injures d'un côté, bravades de l'autre, imprécations des deux parts ; mais, à un signe du capitaine, je vis les coups de bâton pleuvoir au hasard dans les charrettes, sur les épaules ou sur les têtes, et tout rentra dans cette espèce de calme extérieur qu'on appelle l'ordre* ».

¹⁰ (B.) CAZENEUVE et (G.) FARDE, *La lutte antiterroriste*, Paris, PUF, coll. Savoirs, 2023, p. 20.

nombreux blessés »¹¹ en France. De plus, à la suite de l'attentat d'Arras du 13 octobre 2023, la Première ministre Elisabeth Borne a relevé le niveau du plan Vigipirate au niveau « Urgence Attentat » sur l'ensemble du territoire national. C'est dans ce contexte que vont se tenir les Jeux Olympiques et Paralympiques à l'été 2024. Les craintes d'actes de terrorisme sont extrêmement grandes avec des menaces diverses comme par exemple le risque nucléaire, radiologique, bactériologique et chimique (N.R.B.C)¹², le risque d'attentats à la bombe ou des tueries de masse ainsi que la menace de cyberterrorisme¹³. C'est à cette fin de lutter contre le terrorisme qu'est intervenue l'entrée en vigueur de la loi du 19 mai 2023¹⁴. Cette loi comporte toute une série de dispositions sécuritaires dans son chapitre III - article 9 à 19 de la loi - notamment l'article 10. L'intérêt de ces dispositions repose sur le fait qu'il s'agit de la première expérimentation de l'intelligence artificielle à grande échelle en France en matière de vidéoprotection. Cette expérimentation va donc conditionner le futur des caméras « augmentées » en France notamment afin de déterminer un cadre juridique qui repose sur les critères de proportionnalité et de nécessité.

L'article 10 de cette loi prévoit, à titre expérimental, le recours à un traitement algorithmique permettant l'analyse en temps réel des images collectées par des systèmes de vidéoprotection ainsi que sur des caméras installées sur des aéronefs. Autrement dit, cet article porte sur des caméras « augmentées ». Cette qualification provient de la Commission nationale de l'informatique et des libertés (ci-après CNIL). Cette dernière définit les caméras « augmentées » comme un dispositif ayant pour finalité « de catégoriser et d'analyser grâce à l'intelligence artificielle sans identifier une personne de manière unique »¹⁵. Concrètement, il s'agit d'un dispositif d'intelligence artificielle qui

¹¹ L'état de la menace terroriste en France, site de la DGSI : <https://www.dgsi.interieur.gouv.fr/la-dgsi-a-vos-cotes/lutte-contre-terrorisme/letat-de-la-menace-terroriste-en-france> (consulté le 02 mars 2024).

¹² (I.) GALATAS et (J.) MARS, « Paris 2024 : cérémonie d'ouverture des Jeux olympiques – Innovante ? Oui ! Sécurisée (CBRNe/NBCe) ? Non ! », ESKA, in Sécurité globale 2022/4, n° 32, 2022, p. 35 à 49.

¹³ Cheffe d'escadron (M.) CESZNIIEWSKI : cheffe du bureau Gestion de crise cyber au commandement de la gendarmerie dans le cyberspace, Colloque MBA Management de la sécurité du 29 février 2024, Sécuriser l'évènement: l'IA est-elle la martingale absolue ?, <https://www.youtube.com/watch?v=N46xZEa0-ds> (à 3h17 de vidéo), consulté le 02 mars 2024. « La menace cyber est identifiée comme une menace majeure pour les JO 2024. Les derniers Jeux de Tokyo en 2021, c'est pratiquement 4 milliards d'attaques recensées ».

¹⁴ Loi, n° 2023-380, 19 mai 2023 *relative aux Jeux Olympiques et Paralympiques et portant diverses autres dispositions*.

¹⁵ Annexe I: Synthèse des contributions concernant la consultation publique relative aux caméras intelligentes augmentées, établie par la CNIL en juillet 2022.

sera implanté dans les caméras de vidéoprotection¹⁶ ainsi que sur les aéronefs¹⁷ existants, ou dans une nouvelle génération de caméras intelligentes, afin de traiter toutes les images collectées, en temps réel, et de détecter toute situation qui serait jugée anormale par l'algorithme. Cette expérimentation n'a pas été considérée comme une simple évolution technique de l'outil de protection¹⁸ mis en oeuvre par les autorités publiques, mais bien comme un changement d'échelle qui, intrinsèquement, portait atteinte aux libertés fondamentales¹⁹ garanties par l'article 34 de la Constitution. Cette évolution supposait donc l'intervention du législateur. L'autorisation du recours aux caméras « augmentées » a « ravivé les tensions traditionnelles qui existent en matière de déploiement des dispositifs vidéo dans l'espace public »²⁰.

Outre l'aspect sécuritaire qui est un devoir fondamental de l'Etat et requiert donc le recours à toutes les ressources nécessaires²¹, l'aspect lié aux libertés est tout aussi fondamental. En effet, cette expérimentation de l'intelligence artificielle dans le maintien de l'ordre public²² pose de nouvelles questions concernant le respect des libertés fondamentales des personnes, tant individuelles que collectives. Toutefois, les garanties classiques de protection des libertés fondamentales s'appliquent à cette expérimentation. De même, la CNIL veille au respect des droits des personnes dans le domaine du numérique, la loi du 19 mai 2023 a permis d'unifier le régime

¹⁶ Conformément au Titre V « Vidéoprotection » du Livre II « Ordre et sécurité publics » du Code de la sécurité intérieure.

¹⁷ Conformément au Chapitre II « Caméras installées sur les aéronefs », du Titre IV « Caméras mobiles » du Livre II du CSI.

¹⁸ Depuis la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, le législateur parle de systèmes de « vidéoprotection » et non plus de « vidéosurveillance ».

¹⁹ (A.) CANAYER, rapport n° 248 du Sénat sur le projet de loi relatif aux jeux Olympiques et Paralympiques de 2024, 18 janvier 2023, p. 46.

²⁰ (E.) SERUGA-CAU, « L'utilisation de « caméras augmentées » dans l'espace public ou comment innover sans (trop) surveiller », *Communication - Commerce électronique*, Lexisnexis, n° 78, juillet-août 2023, p. 1.

²¹ Article L.111-1 du CSI : « La sécurité est un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives. / L'Etat a le devoir d'assurer la sécurité en veillant, sur l'ensemble du territoire de la République, à la défense des institutions et des intérêts nationaux, au respect des lois, au maintien de la paix et de l'ordre publics, à la protection des personnes et des biens. / Il associe à la politique de sécurité, dans le cadre de dispositifs locaux dont la structure est définie par voie réglementaire, les collectivités territoriales et les établissements publics de coopération intercommunale ainsi que les représentants des professions, des services et des associations confrontés aux manifestations de la délinquance ou œuvrant dans les domaines de la prévention, de la médiation, de la lutte contre l'exclusion ou de l'aide aux victimes ».

²² L'ordre public comprend la sûreté, la sécurité et la salubrité conformément à l'article L.2212-2 du Code Général des Collectivités Territoriales. Il comprend également la dignité humaine comme l'a précisé le Conseil d'État (CE, Ass., 27 octobre 1995, n° 13672, *Commune de Morsang-sur-Orge, Leb*).

juridique de la vidéoprotection en soumettant sous son contrôle tous les systèmes de vidéoprotection. L'intelligence artificielle est l'enjeu majeur du XXI^e siècle dans tous les domaines de la société²³, il est possible pour les Etats d'utiliser l'intelligence artificielle afin de renforcer leurs pouvoirs vis-à-vis de leur peuple comme le crédit social chinois qui est un moyen pour l'Etat de classer ses citoyens en fonction de leur score social pour leur attribuer des avantages ou des sanctions. Pour éviter que les usages liés à l'intelligence artificielle ne soient toujours comparés à ceux qui sont liberticides dans les régimes autoritaires l'Europe va bientôt se doter d'une réglementation relative à l'intelligence artificielle. En effet, une proposition de règlement européen sur l'intelligence artificielle a été adoptée le 13 mars 2024 et une entrée en vigueur est prévue pour 2026. Cette réglementation vise à créer un cadre juridique éthique pour le développement et la mise sur le marché d'intelligences artificielles respectueuses des droits et libertés fondamentaux.

Compte tenu du fait qu'une expérimentation des caméras « augmentées » va se dérouler au niveau français et que l'Union européenne se dote d'une réglementation sur l'intelligence artificielle, il convient de se demander comment ces législations vont-elles respecter les droits et libertés fondamentaux tout en assurant un niveau de sécurité suffisant en matière de vidéoprotection.

Pour cela, il convient, en premier lieu, d'étudier le cadre juridique expérimental mis en oeuvre pour le déploiement des caméras « augmentées ». Cette étude permettra également de mettre en exergue les limites liées à leur usage afin de respecter le droit au respect de la vie privée (Titre I). Dans une seconde partie, nous étudierons davantage le renforcement du contrôle non juridictionnel opéré par la CNIL en matière de vidéoprotection intelligentes ou non. Sera également étudié le futur règlement européen tant au regard des lignes rouges qu'il impose aux intelligences artificielles qu'au regard des principes fondamentaux qu'elles doivent respecter (Titre II).

²³ Selon le président de la Fédération de Russie, POUTINE (V.), « l'intelligence artificielle représente l'avenir (...) de toute l'humanité. Elle amène des opportunités colossales et des menaces imprévisibles aujourd'hui ». Il surenchérit en déclarant que « celui qui deviendra leader en ce domaine sera le maître du monde ».

**TITRE I : LE RECOURS EXPÉRIMENTAL AUX CAMÉRAS
« AUGMENTÉES » ET LE RENOUVELLEMENT DE LA QUESTION DE LA
PROTECTION DE LA VIE PRIVÉE**

TITRE I : LE RECOURS EXPÉRIMENTAL AUX CAMÉRAS « AUGMENTÉES » ET LE RENOUVELLEMENT DE LA QUESTION DE LA PROTECTION DE LA VIE PRIVÉE

Il convient, en premier lieu, d'étudier la loi n° 2023-380 du 19 mai 2023 et plus particulièrement son article 10 qui a autorisé le recours, par les pouvoirs publics, à des caméras intelligentes afin de mieux garantir la sécurité. Cet article 10 ne doit pas être considéré comme un blanc-seing au profit des pouvoirs publics pour recourir à cette technologie puisqu'il circonscrit l'usage de celle-ci à des conditions particulièrement strictes, en tout cas dans le texte. En effet, les caméras « augmentées » ne pourront être utilisées que pour assurer la sécurité des manifestations sportives, récréatives et culturelles qui rempliront d'autres critères tenant à l'ampleur de l'évènement ainsi que relativement aux risques encourus pour la sécurité des personnes. Les Jeux Olympiques et Paralympiques sont le parfait exemple d'un tel évènement cumulant à la fois un très grand nombre de spectateurs et des risques accrus de troubles à l'ordre public. Il convient donc de déterminer le cadre juridique dans lequel seront déployées les caméras « augmentées » (Chapitre 1).

Par ailleurs, outre l'aspect sécuritaire lié aux caméras « augmentées », les autorités publiques ont le devoir de préserver les libertés fondamentales individuelles et collectives. En effet, la protection de la vie privée est un enjeu fondamental en matière de numérique, surtout lorsque les technologies sont utilisées à des fins sécuritaires. Les caméras « augmentées » modifient la perception de l'image puisqu'avec celles-ci les personnes ne sont plus uniquement filmées mais elles sont également analysées. Cela oblige donc à accompagner l'expérimentation de garanties nécessaires pour la protection de la vie privée (Chapitre 2).

Chapitre 1 : Le cadre juridique de l'article 10 de la loi du 19 mai 2023 concernant le déploiement des caméras « augmentées »

Le recours à un traitement algorithmique pour traiter les images issues des systèmes de vidéoprotection a supposé la création d'un régime juridique *ad hoc*. En effet, il s'agit d'une innovation juridique il était donc nécessaire de décider dans quelles situations cette technologie pourrait être utilisée. Cette technologie a pour finalité de lutter contre les atteintes les plus graves à l'ordre public et pour des évènements très spécifiques (Section 1).

Par ailleurs, nous étudierons également ce que recouvre juridiquement le terme « d'expérimentation » afin de mieux comprendre les différents scénarios pouvant s'ouvrir à la fin de l'expérimentation des caméras « augmentées », c'est-à-dire la pérennisation de leur déploiement, la modification de leur régime pour une application pérenne ou bien l'abandon pur et simple de cette technologie (Section 2).

Section 1 : L'utilisation des caméras « augmentées » pour lutter contre les atteintes les plus graves à l'ordre public

L'article 10 de la loi du 19 mai 2023 autorise le recours aux caméras « augmentées », c'est-à-dire à des caméras dotées d'une couche logicielle capable de traiter et d'analyser en temps réel les images collectées afin de mieux garantir la sécurité dans l'espace recouvert par ces dispositifs. La loi a circonscrit l'usage des caméras « augmentées » à un certain type d'évènement que sont les manifestations sportives, récréatives et culturelles (Paragraphe 1). Toutefois, l'interprétation de la loi peut permettre de recourir à cette technologie dans un périmètre géographique bien plus étendu qu'au simple lieu où se tient l'évènement (Paragraphe 2).

Paragraphe 1 : Le recours aux caméras « augmentées » afin de sécuriser les « manifestations » sportives, récréatives et culturelles

L'article 10 de la loi du 19 mai 2023 prévoit le recours aux caméras « augmentées » pour la seule sécurisation des « manifestations » sportives, récréatives et culturelles. Il convient donc de définir précisément ce que recouvre juridiquement ces manifestations (A). Néanmoins, la loi prévoit d'autres critères permettant d'encadrer l'usage de telles caméras prenant en compte le contexte lié à la tenue de l'évènement, cela va donc réduire les possibilités de recourir aux caméras « augmentées » par les autorités publiques (B).

A. La limite matérielle de l'expérimentation des caméras « augmentées » aux seules « manifestations » sportives, récréatives et culturelles

Il n'existe aucune définition légale ou réglementaire du concept de « manifestation ». Les textes, comme par exemple le décret-loi du 23 octobre 1935, se contentent de préciser le régime juridique de la manifestation en la soumettant à une obligation de déclaration préalable²⁴. C'est la jurisprudence qui a pu précisément définir la manifestation comme : « tout rassemblement, statique ou mobile, sur la voie publique d'un groupe organisé de personnes aux fins d'exprimer collectivement et publiquement une opinion ou une volonté commune »²⁵. En plus de se dérouler sur la voie publique, la manifestation suppose un groupe organisé de personnes qui expriment une opinion de manière collective. Toutefois, les « manifestations sportives, récréatives et culturelles » auxquelles fait référence le premier paragraphe de l'article 10 de la loi du 19 mai 2023 ne peuvent être assimilées à ce genre de manifestation ayant pour dessein d'exprimer des opinions comme par exemple une opinion politique²⁶. Ces manifestations peuvent se définir comme « un évènement

²⁴ Article 1er du décret-loi du 23 octobre 1935 portant réglementation des mesures relatives au renforcement du maintien de l'ordre public: « Les réunions sur la voie publique sont et demeurent interdites dans les conditions prévues par la loi du 30 juin 1881, article 6. / **Sont soumis à l'obligation d'une déclaration préalable, tous cortèges, défilés et rassemblements de personnes, et, d'une façon générale, toutes manifestations sur la voie publique.** / Toutefois, sont dispensées de cette déclaration les sorties sur la voie publique conformes aux usages locaux ».

²⁵ Cass, Crim, 9 févr. 2016, n° 14-82.234.

²⁶ (O.) FILLIEULE, « Stratégies de la rue », Paris, Presses de Sciences Po, 1997, p. 44, *in* (O.) FILLIEULE et (D.) TARTAKOWSKY, *La manifestation*, Presses de Sciences Po, 2013, 224 p.

attirant un public extrêmement large »²⁷ dans un but autre que celui d'exprimer une opinion commune. De même, les manifestations sportives, récréatives et culturelles sont à distinguer des rassemblements à caractère festif et musical²⁸, ces derniers n'étant pas non plus intégrés dans l'expérimentation des caméras « augmentées ».

Les manifestations sportives, récréatives et culturelles sont donc, d'un point de vue juridique, davantage des évènements que des manifestations. Dès lors, la liberté de manifestation ne pourra sans doute pas être recevable pour contester devant le juge administratif le déploiement des caméras « augmentées » lors des JOP 24. Ces évènements sont plus ou moins importants selon leur taille ou leur renommée. Ils font l'objet d'un régime juridique spécifique, lequel est renforcé dès que l'évènement dépasse 1.500 personnes²⁹. Ces événements concentrent généralement une très grande masse de personnes, par exemple le Stade de France peut accueillir aux alentours de 80.000 personnes selon l'évènement. La sécurité doit donc être renforcée pendant ceux-ci et cela sera d'autant plus important lors des Jeux Olympiques et Paralympiques 2024, lesquels accueilleront pas moins de 15.000 athlètes et plus de 13 millions de spectateurs³⁰.

Néanmoins, l'expérimentation des caméras « augmentées » ne concerne pas l'ensemble des manifestations sportives, récréatives et culturelles puisque la loi prévoit d'autres conditions restrictives afin de circonscrire l'usage de cette technologie aux seuls évènements se déroulant dans un contexte particulier.

²⁷ Définition du dictionnaire Larousse.

²⁸ Article L.211-5 et suivants du CSI.

²⁹ Article R.211-22 du CSI: « Les organisateurs de manifestations sportives, récréatives ou culturelles à but lucratif dont le public et le personnel qui concourt à la réalisation de la manifestation peuvent atteindre plus de 1 500 personnes, soit d'après le nombre de places assises, soit d'après la surface qui leur est réservée, sont tenus d'en faire la déclaration au maire, à Paris, ou sur les emprises des aéroports de Paris-Charles de Gaulle, Paris-Le Bourget et Paris-Orly au préfet de police et, dans le département des Bouches-du-Rhône, au préfet de police des Bouches-du-Rhône. / La déclaration peut être souscrite pour une seule ou pour plusieurs manifestations dont la programmation est établie à l'avance. / La déclaration est faite un an au plus et, sauf urgence motivée, un mois au moins avant la date de la manifestation ».

³⁰ Exposé des motifs de la loi n°2023-380 du 19 mai 2023 relative aux Jeux Olympiques et Paralympiques et portant diverses autres dispositions.

B. Le recours aux caméras « augmentées » pour prévenir les atteintes les plus graves à l'ordre public

Depuis la loi du 30 octobre 2017³¹, afin de mieux sécuriser les événements qui rassemblent un très grand nombre de personnes, il est possible de recourir à des périmètres de protection - dit périmètres SILT -. Ces périmètres SILT sont institués par le représentant de l'Etat dans le département³², lequel va définir les règles d'accès et de circulation au sein de ce périmètre afin d'assurer la sécurité de l'évènement « exposé à un risque d'acte de terrorisme en raison de sa nature et de l'ampleur de sa fréquentation »³³. Dans son avis relatif au projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme³⁴, le Conseil d'État estime que la mise en oeuvre de tels périmètres est adaptée entre la prévention des atteintes à l'ordre public et le droit au respect de la vie privée des personnes. Les périmètres SILT seront évidemment utilisés afin de sécuriser les différentes épreuves des JOP 24 comme le montrent les différents plans des sites olympiques sur le site internet de la Préfecture de police³⁵.

Depuis 2017 la sécurisation des grands événements est un enjeu majeur pour les autorités publiques et la loi du 19 mai 2023 s'inscrit dans cette lignée avec le déploiement des caméras « augmentées ». Elles visent à « mieux garantir la sécurité »³⁶ des manifestations sportives, récréatives et culturelles qui sont susceptibles de faire face aux atteintes les plus graves à l'ordre public. L'article 10 de cette loi prévoit le recours à celles-ci afin de sécuriser des événements qui « sont particulièrement exposés à des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes ». Ces dispositifs visent donc à prévenir le haut du spectre dans les atteintes à l'ordre public. Le Conseil constitutionnel a confirmé cette perspective dans sa décision du 17 mai 2023

³¹ Loi, n° 2017-1510, 30 octobre 2017 *renforçant la sécurité intérieure et la lutte contre le terrorisme*.

³² Article L.226-1 du code de la sécurité intérieure.

³³ *Ibid.*

³⁴ CE, avis, 15 juin 2017, n° 393348, projet de loi relatif à la prorogation de certaines mesures de lutte contre le terrorisme du code de la sécurité intérieure.

³⁵ Annexe II : Plan de sécurisation des sites olympiques issu du site internet de la Préfecture de police de Paris.

³⁶ Titre du chapitre III de la loi n°2023-380 du 19 mai 2023.

portant sur la loi relative aux Jeux Olympiques³⁷ puisqu'il interprète la loi comme excluant le recours à de tels dispositifs pour les seules atteintes aux biens³⁸.

Il y a donc une multiplication des règles spéciales concernant ces évènements qui rassemblent beaucoup de personnes afin d'assurer leur sécurité face au risque terroriste. Néanmoins, outre ces deux critères, la loi prévoit que sont seuls concernés les évènements ayant une fréquentation d'ampleur ou lorsque les circonstances font que la tenue de l'évènement présente des risques de troubles graves à l'ordre public³⁹. Ces critères vont permettre la désignation de cet évènement en tant que « grand évènement ». Cette qualification juridique va permettre aux pouvoirs publics d'étendre le déploiement des caméras « augmentées » au-delà du seul lieu où se déroule l'évènement.

³⁷ Cons. const., 17 mai 2023, n° 2023-850 DC, *Loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions*.

³⁸ *Ibid*, considérant 37: « En deuxième lieu, les dispositions contestées prévoient que les traitements algorithmiques des images ainsi collectées ne peuvent être mis en œuvre qu'afin d'assurer la sécurité de manifestations sportives, récréatives ou culturelles qui, par l'ampleur de leur fréquentation ou par leurs circonstances, sont particulièrement exposées à des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes. Elles réservent ainsi l'usage de tels traitements à des manifestations présentant des risques particuliers d'atteintes graves à l'ordre public et **en excluent la mise en œuvre en cas de seuls risques d'atteintes aux biens** ».

³⁹ Comme par exemple les matchs de football entre supporters rivaux donnant lieu à des incidents graves hors du stade comme le caillasse du bus de l'Olympique Lyonnais avant le match contre l'Olympique de Marseille le 29 octobre 2023, https://www.francetvinfo.fr/sports/foot/football-avec-la-multiplication-recente-des-violences-hors-des-stades-le-hooliganisme-resurgit-il-pour-autant-en-france_5450203.html (consulté le 23 février 2024).

Paragraphe 2 : La qualification de « grand évènement » des jeux Olympiques permettant d'étendre le périmètre géographique de déploiement des caméras « augmentées »

Le déploiement de ces caméras peut se faire aux abords immédiats du lieu où se tient l'évènement, comme le prévoit la loi. Toutefois, les Jeux Olympiques et Paralympiques ont été désignés « grand évènement » par décret⁴⁰. Dès lors, le régime juridique des grands évènements va s'appliquer et permettre le déploiement des caméras « augmentées » dans les lieux qui sont communément appelés « fan-zones » (A). Ce premier élément va permettre d'étendre considérablement le périmètre géographique de déploiement des caméras « augmentées ». Par ailleurs, l'article 10 de la loi du 19 mai 2023 prévoit quant à lui la possibilité d'utiliser ces dispositifs de vidéoprotection pour sécuriser différents lieux qui vont desservir le lieu où se tient l'évènement en cause (B).

A. Le recours aux caméras « augmentées » pour sécuriser les lieux connexes à l'évènement susceptible de faire l'objet d'un acte de terrorisme

Juridiquement, un « grand évènement » est désigné par décret conformément à l'article L.211-11-1 du code de la sécurité intérieure⁴¹. Tel fut le cas par exemple de la coupe du monde de rugby 2023⁴². Les JOP 24 seront une période de très grands rassemblements de personnes, il s'agira d'un grand évènement sportif et économique, il s'agit également un grand évènement d'un point de vue juridique. Cette qualification de « grand évènement » pour les JOP 24 permet à l'autorité de police dans le département, et le préfet de police dans la région Ile-de-France⁴³, de déployer ces nouvelles caméras « augmentées » dans des lieux connexes à l'évènement, les « fans-zones ». En

⁴⁰ Décret n° 2021-1397 du 27 octobre 2021 portant application de l'article L. 211-11-1 du code de la sécurité intérieure aux jeux Olympiques et Paralympiques de 2024.

⁴¹ Article modifié par l'article 15 de la loi du 19 mai 2023 n°2023-380.

⁴² Décret n° 2023-847 du 30 août 2023 portant application de l'article L. 211-11-1 du code de la sécurité intérieure aux « villages rugby » de la Coupe du monde de rugby 2023 et modifiant le décret du 22 décembre 2022 portant application de l'article L. 211-11-1 du code de la sécurité intérieure à la Coupe du monde de rugby 2023, JORF n°0202 du 1er septembre 2023.

⁴³ Article 14 de la loi n°2023-380 *op. cit.*

effet, les « fans-zones » peuvent se définir comme des lieux où les personnes comme des supporters se réunissent pour assister en direct à la retransmission d'un évènement sportif. Juridiquement ces fan-zones entrent dans le champ d'application de l'article L.211-11-1 du Code de la sécurité intérieure. Cette qualification de « grand évènement » ne peut, toutefois, s'appliquer qu'aux évènements « exposés à un risque d'actes de terrorisme en raison de leur nature et de l'ampleur de leur fréquentation »⁴⁴. Les JOP 24 étant susceptibles de faire l'objet d'actes de terrorisme, toutes les fan-zones sont également susceptibles de faire l'objet de tels actes. Par conséquent les caméras « augmentées pourront être déployées en leur sein ainsi qu'à leurs abords immédiats sur la voie publique. Cela va donc grandement accroître la zone de déploiement de ces nouvelles caméras puisque pendant cette période il est prévu environ 200 fan-zones en France⁴⁵. Il est donc probable qu'une épreuve des JOP 24 se déroulant sur Paris, qu'une fan-zone se trouvant à Marseille et qu'il faille déployer les caméras « augmentées » à la fois à Paris et à Marseille puisque le lien entre les deux évènements est incontestable.

De par cette interprétation de l'article 10 de la loi JOP, le caractère restrictif du déploiement des caméras « augmentées » est contestable puisqu'il est possible de considérer que tous les évènements connexes à cet évènement pourront être soumis au recours de ces nouvelles technologies afin d'accroître la sécurité dans sa globalité. Par ailleurs, la loi prévoit le déploiement des caméras « augmentées » dans les lieux publics desservant les lieux des évènements, ce qui accroît encore le périmètre géographique des caméras « augmentées ».

⁴⁴ Article L.211-11-1 du CSI.

⁴⁵ « Paris 2024 : 197 projets de fan-zones Club 2024, mais l'initiative est boudée par quelques grandes villes », Le Monde, publié le 19 janvier 2024.

B. Le déploiement des caméras « augmentées » dans les lieux publics desservant le lieu de l'évènement

Le premier paragraphe de l'article 10 de la loi JOP prévoit le déploiement des caméras à traitement algorithmique « dans les véhicules et les emprises de transport public et sur les voies les desservant ». Cette nouvelle hypothèse va également élargir de manière considérable le périmètre géographique couvert par ces nouvelles caméras de vidéoprotection afin de mieux garantir la sécurité des manifestations sportives, récréatives et culturelles. En effet, il a été précisé plus haut que les caméras « augmentées » peuvent être déployées sur le lieu de l'évènement ainsi que sur les « fan-zones » puisqu'il s'agit d'un événement en lien avec le premier. Dès lors, en poursuivant cette logique il sera donc possible de déployer les caméras « augmentées » sur les emprises de transport public et sur les voies desservant à la fois le lieu de l'évènement et le lieu où se situe la « fan-zone ».

Pour mieux comprendre cette hypothèse il est possible de prendre de nouveau l'exemple du Stade de France. Ce dernier a été désigné stade olympique et va donc naturellement accueillir plusieurs épreuves olympiques et paralympiques⁴⁶. Il faut donc organiser l'accueil et le départ de près de 80.000 spectateurs que le stade peut accueillir et le recours aux caméras « augmentées » pourra être possible dans le stade et à ses abords mais également dans le périmètre géographique plus étendu de l'article 10 précité afin de garantir la sécurité des personnes. Pour cela, le Stade de France est desservi par les gares « Stade de France Saint-Denis » (RER D), « La Plaine Stade de France » (RER B), et « Saint-Denis Porte de Paris » (Métro 13), ces emprises de transport public pourront donc accueillir ces nouveaux dispositifs de vidéoprotection. Par ailleurs, pour faciliter le flux des spectateurs dans les transports, les organisateurs informent les spectateurs qu'ils peuvent également se reporter sur d'autres gares qui sont : la future station « Pleyel » (Métro 14), la station « Front Populaire » (Métro 12) ou la gare « Saint-Denis » (Train H depuis la gare du Nord à Paris), la sécurité devra donc également être assurée dans ces gares et cela va élargir le périmètre géographique d'utilisation des caméras « augmentées »⁴⁷. De même, il sera juridiquement possible

⁴⁶ Informations issues du site Paris 2024: <https://www.paris2024.org/fr/site/stade-de-france/> (consulté le 23 février 2024).

⁴⁷ Annexe III : Carte du site olympique du Stade de France comprenant les potentiels emplacements des caméras « augmentées ».

de déployer les caméras « augmentées » dans tous les lieux de transport public desservant les fan-zones en France si cela est jugé nécessaire et proportionné au but recherché, puisque ces dernières sont des évènements connexes à l'évènement qu'il convient de sécuriser en ayant recours aux caméras « augmentées ».

Par conséquent, le périmètre géographique couvert par les caméras « augmentées » pourra être extrêmement étendu si la menace le requiert. Cela pourrait donc renforcer les idées des opposants au recours aux nouvelles technologies en matière de sécurité et renforcer leur position qui consiste à dire que cette technologie va « créer un gigantesque système de ciblage d'anomalies »⁴⁸ puisque son périmètre de déploiement pourra être étendu.

Malgré une possible extension du périmètre géographique de déploiement des caméras « augmentées » selon la gravité de la menace, il convient de constater que l'article 10 de la loi du 19 mai 2023 prévoit d'autres limites relatives à leur recours. En effet, ces dispositifs sont soumis au régime juridique de l'expérimentation et l'article 10 prévoit explicitement des limites concernant les usages possibles des caméras « augmentées ».

Section 2 : Les limites tenant à l'usage des caméras « augmentées »

Précédemment a été étudié le contexte dans lequel vont pouvoir se déployer les caméras « augmentées », à cette occasion ont été mises en évidence plusieurs limites d'ordre matérielles. Pour rappel, ces dispositifs peuvent uniquement être mis en oeuvre pour assurer la sécurité de certaines manifestations sportives, récréatives et culturelles. Ces dernières faisant l'objet de menaces particulièrement graves pour l'ordre public et la sécurité des personnes.

Désormais, il convient d'étudier d'autres limites concernant le dispositif juridique mis en place par l'article 10 de la loi du 19 mai 2023. Tout d'abord, le traitement algorithmique des images collectées par les caméras de vidéoprotection et les aéronefs est une disposition expérimentale. Cette « expérimentation » repose sur un régime juridique issu de la Constitution qu'il conviendra d'étudier afin de mieux comprendre son encadrement et sa portée (Paragraphe 1). Par ailleurs, la loi du 19 mai 2023 elle-même, prévoit des limites tenant au recours de cette technologie en empêchant

⁴⁸ La Quadrature du Net: <https://www.laquadrature.net/biometrie-jo/> (consulté le 13 mars 2024).

de recourir aux données biométriques et à la reconnaissance faciale ainsi que de cantonner cette technologie à un rôle d'aide à la décision (Paragraphe 2).

Paragraphe 1 : L'encadrement juridique des normes expérimentales

Le cadre juridique de l'expérimentation est d'origine constitutionnelle. Dès lors, la Constitution octroie la possibilité aux pouvoirs législatifs et réglementaires d'adopter des législations temporaires. Toutefois, ce régime juridique ne remet pas en cause les matières dévolues au pouvoir législatif et celles dévolues au pouvoir réglementaire. Comme l'expérimentation des caméras « augmentées » était conçue comme portant atteinte en elle-même aux libertés fondamentales une loi a dû être adoptée ce qui représente une limite formelle à l'expérimentation (A). Par ailleurs, une expérimentation étant intrinsèquement temporaire, la Constitution pose cette condition de temporalité. Ce délai va être déterminant concernant les suites à donner à l'expérimentation des caméras « augmentées » (B).

A. La limite formelle à l'expérimentation du recours aux caméras « augmentées »

Introduits par la loi constitutionnelle n° 2003-276 du 28 mars 2003 relative à l'organisation décentralisée de la République, les articles 37-1 et 72 de la Constitution autorisent l'adoption de normes expérimentales. La distinction à opérer entre ces deux régimes juridiques est relative à « la dévolution d'une partie du pouvoir normatif de l'Etat »⁴⁹. Autrement dit, lorsque le pouvoir législatif autorise les collectivités territoriales à adopter des normes expérimentales c'est l'article 72 de la Constitution qui sera utilisé. A l'inverse, lorsque la mise en oeuvre de l'expérimentation repose uniquement sur le législateur ou le pouvoir réglementaire il faut recourir à l'article 37-1 de la Constitution⁵⁰. En tout état de cause, l'expérimentation repose sur l'observation de comportements

⁴⁹ (J.-H.) STAHL, « L'expérimentation en droit français : une curiosité en mal d'acclimatation », *Revue juridique de l'économie publique* n° 681, 2010, étude 11, paragraphe 23.

⁵⁰ Article 37-1 de la Constitution: « La loi et le règlement peuvent comporter, pour un objet et une durée limités, des dispositions à caractère expérimental ».

particuliers ainsi que sur leur évaluation afin d'adopter des normes générales⁵¹. Cela s'inscrit en rupture avec la tradition juridique française et le principe d'égalité qui suppose l'adoption de normes générales afin de réglementer les comportements particuliers⁵². Malgré tout, il est remarquable de constater que toutes les expérimentations menées depuis les années 70 ne représentent qu'une infime partie de la législation française⁵³. Les conditions posées par l'article 37-1 de la Constitution sont identiques qu'il s'agisse du législateur ou du pouvoir réglementaire. Le régime juridique de l'expérimentation est l'exemple typique de la théorie dynamique des normes développée par H. KELSEN, selon laquelle une norme inférieure est conforme à la norme supérieure, quel que soit son contenu, dès lors qu'elle respecte la procédure instaurée par la norme supérieure. Autrement dit, la norme supérieure est une simple norme de compétence et n'impose aucun contenu précis à la norme inférieure.

C'est sur la base de cet article 37-1 que le recours expérimental au traitement algorithmique des images collectées par les caméras de vidéoprotection et aéronefs a été autorisé à l'article 10 de la loi JOP. Celle-ci a pu être déclarée conforme à la Constitution par le Conseil constitutionnel dans sa décision du 17 mai 2023⁵⁴ puisqu'elle respecte, selon lui, les conditions qu'il avait pu dégager au fil de sa jurisprudence relative à l'expérimentation. En effet, dans sa décision du 12 août 2004⁵⁵, le Conseil constitutionnel confirme le principe de l'expérimentation tout en rappelant les limites imposées à celle-ci puisqu'elle doit respecter un objet et une durée limités. L'article 10 de la loi du 19 mai 2023 se fonde expressément sur l'article 37-1 de la Constitution puisqu'il autorise à « titre expérimental » le recours au traitement algorithmique des images collectées par les caméras de vidéoprotection et les aéronefs. Le recours à une loi pour cette expérimentation a été jugé utile par différents acteurs comme la CNIL qui parle d'une « modification de nature [des caméras de

⁵¹ Cons. const., 28 juillet 1993, n° 93-322 DC, *Loi relative aux établissements publics à caractère scientifique, culturel et professionnel*, considérant 9: « Considérant qu'il est même loisible au législateur de prévoir la possibilité d'expériences comportant des dérogations aux règles ci-dessus définies de nature à lui permettre d'adopter par la suite, au vu des résultats de celles-ci, des règles nouvelles appropriées à l'évolution des missions de la catégorie d'établissements en cause ; [...] elles doivent faire l'objet d'une évaluation conduisant à leur maintien, à leur modification, à leur généralisation ou à leur abandon ; ».

⁵² (J.-É.-M.) PORTALIS, Discours préliminaire sur le projet de Code civil, 1er Pluviôse an IX (21 janvier 1801) : « En effet, la loi statue sur tous : elle considère les hommes en masse, jamais comme particuliers ».

⁵³ (J.-H.) STAHL, « L'expérimentation en droit français, » *op. cit.*, paragraphe 67.

⁵⁴ Cons. const., 17 mai 2023, n° 2023-850 DC, *op. cit.*

⁵⁵ Cons. const., 12 août 2004, n° 2004-503 DC, *Loi relative aux libertés et responsabilités locales*, considérants 8 et suivants.

vidéoprotection] »⁵⁶. Les caméras « augmentées » sont considérées comme portant intrinsèquement atteinte aux libertés fondamentales ce qui a justifié le recours à une loi conformément à l'article 34 de la Constitution⁵⁷. Toutefois, il est à noter que des traitements algorithmiques d'images collectées par les caméras de vidéoprotection sont déjà utilisés par les autorités publiques tel que le système de lecture automatisé des plaques d'immatriculation ou bien par des entreprises telles que la SNCF qui a pu expérimenter depuis 2017 l'usage d'algorithmes afin d'assurer la sécurité des personnes en détectant des « objets abandonnés ou des mouvements anormaux »⁵⁸. Autrement dit, bien que cette expérimentation soit innovante il ne s'agit pas de la première utilisation de l'intelligence artificielle pour le traitement d'images collectées par les caméras de vidéoprotection. Cette expérimentation est la première à une si grande échelle géographique.

En plus d'une limitation concernant le recours aux caméras « augmentées » aux seules très grandes manifestations sportives, récréatives et culturelles, l'adoption de cette expérimentation a également supposé qu'un délai soit fixé afin de limiter celle-ci dans le temps.

B. La limitation temporelle de cette expérimentation

Cette limite semble aller de soi mais l'article 37-1 de la Constitution précise que l'expérimentation est à durée limitée. Cette expression confine à la tautologie comme le relève le conseiller d'État Jacques-Henri STAHL puisque « une expérimentation, sauf à ne plus en être une, ne saurait, effectivement, être [...] pérenne »⁵⁹. Cette limite temporelle imposée à l'expérimentation est contrôlée par le Conseil constitutionnel. En effet, ceci peut être un motif de déclaration d'inconstitutionnalité lorsqu'il constate que le législateur délègue au pouvoir réglementaire le soin

⁵⁶ CNIL, position sur les conditions de déploiement des caméras dites « intelligentes » ou « augmentées » dans les espaces publics, juillet 2022, p. 9.

⁵⁷ Article 34 de la Constitution: « La loi fixe les règles concernant : - les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques [...] ».

⁵⁸ (G.) VUILLETET, rapport n° 939 sur le projet de loi, adopté par le Sénat, après engagement de la procédure accélérée relatif aux JOP 24 et portant diverses autres dispositions, 9 mars 2023, p.63 *in* (C.) CASTETS-RENARD et (A.) TURCI, « 'Caméras augmentées' : un danger pour les libertés lors des Jeux Olympiques et Paralympiques (et au-delà) ? », *Recueil Dalloz*, numéro 22, 2023.

⁵⁹ (J.-H.) STAHL, « L'expérimentation en droit français » *op. cit.*, paragraphe 29.

de fixer le terme de l'expérimentation. Par exemple, dans sa décision du 16 juillet 2009⁶⁰ le Conseil constitutionnel a censuré les différentes expérimentations prévues par la loi parce que le législateur n'avait pas fixé lui-même la durée maximale de l'expérimentation. Par ailleurs, le Conseil d'État en tant que conseil du Gouvernement va contrôler la durée de l'expérimentation et va notamment regarder si celle-ci n'est pas excessive, la durée de l'expérimentation devant être « strictement nécessaire »⁶¹.

Concernant l'expérimentation des caméras « augmentées », l'article 10 de la loi JOP détermine, dès ses premiers mots, que l'expérimentation se déroulera jusqu'au 31 mars 2025. Cette durée limite a été débattue au Parlement puisque l'article 7 du projet de loi déposé à la fin d'année 2022 prévoyait une expérimentation des caméras « augmentées » jusqu'au 30 juin 2025⁶². Outre la date de fin, l'expérimentation pouvait débuter dès l'entrée en vigueur de la loi et les caméras « augmentées » pouvaient donc être utilisées pendant la Coupe du monde de Rugby 2023 mais cela ne fut pas le cas puisque les premiers essais ont débuté les 3 et 5 mars 2024 avec un concert de Dépêche Mode⁶³. Toutefois, un rapport sénatorial du 10 avril 2024 préconise de recourir à davantage d'expérimentation de cette technologie afin qu'elle soit prête pour les JOP 24 puisque « une seule expérimentation de cette technologie, sur six caméras et quatre cas d'usages, au bénéfice de la seule préfecture de police de Paris avait été réalisée plus d'un an après la promulgation de la loi l'autorisant »⁶⁴.

L'article 10 de la loi JOP prévoit un autre délai, plus court cette fois, puisque le paragraphe XI prévoit qu'un rapport d'évaluation de cette expérimentation doit être rendu par le Gouvernement au Parlement et à la CNIL au plus tard le 31 décembre 2024. Le délai dans lequel s'insère l'évaluation prouve immédiatement que cette expérimentation n'a qu'un seul but : assurer la sécurité des Jeux Olympiques et Paralympiques. Elle n'a sans doute pas vocation à s'appliquer à

⁶⁰ Cons. const., 16 juillet 2009, n° 2009-584 DC, *Loi portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires*, considérant 39.

⁶¹ CE, avis consultatif, 27 novembre 2017, n° 393744, portant sur le projet de loi pour un Etat au service d'une société de confiance.

⁶² Projet de loi, n° 220, relatif aux Jeux Olympiques et paralympiques 2024, 22 décembre 2022.

⁶³ Le Figaro, article publié le 02 mars 2024, <https://www.lefigaro.fr/actualite-france/jo-paris-2024-cameras-intelligentes-concert-depeche-mode-bercy-20240216> (consulté le 16 mars 2024).

⁶⁴ (A.) CANAYER et (M.-P.) de LA GONTRIE, n° 527, 10 avril 2024, rapport d'information sur l'application de la loi du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions ».

d'autres types d'évènements pour le moment, sauf à être expérimentée pour que cette technologie soit opérationnelle pour les JOP 24. Cette évaluation est primordiale puisqu'il s'agit d'évaluer l'efficacité d'un dispositif expérimental pour savoir s'il faut le pérenniser tel qu'il est, le modifier ou bien l'abandonner. L'évaluation reste à la base de l'expérimentation puisque sans cette évaluation l'expérimentation n'a que peu d'intérêt la voie législative classique semblant en ce cas plus adéquate. Le Conseil constitutionnel a en outre rappelé que l'évaluation de cette expérimentation devait prendre en compte « les atteintes portées au droit au respect de la vie privée [et] tenir compte de son efficacité dans la prévention des atteintes à l'ordre public »⁶⁵. De même, Émilie SERUGA-CAU espère que les autorités sauront renoncer à pérenniser cet outil si l'évaluation n'est pas satisfaisante, et ce malgré les investissements consentis⁶⁶. Néanmoins, en matière de sécurité il y a un « effet-cliquet » très important et beaucoup de dispositions ayant initialement une vocation temporaire se retrouvent pérennisés, comme par exemple les périmètres SILT évoqués plus haut. Il est donc fort probable que les caméras « augmentées » s'inscrivent durablement dans le paysage juridique français.

Malgré ces limites juridiques tenant à l'expérimentation des caméras « augmentées », la loi JOP prévoit d'autres limites relatives à l'usage de ces caméras ainsi qu'à la conception des traitements algorithmiques.

⁶⁵ Cons. const., 17 mai 2023, *op. cit.*, considérant 48.

⁶⁶ (E.) SERUGA-CAU, « L'utilisation de « caméras augmentées » dans l'espace public ou comment innover sans (trop) surveiller », *op. cit.*

Paragraphe 2 : Les limites relatives à la conception et l'utilisation des caméras « augmentées »

Outre les limites relatives au régime juridique de l'expérimentation, l'article 10 de la loi JOP a conditionné le recours aux caméras « augmentées » de deux manières. Tout d'abord, l'article interdit explicitement, dans son paragraphe IV, le traitement de données biométriques et le recours à la reconnaissance faciale (A). Néanmoins, il est possible de s'interroger sur l'interdiction de traiter des données biométriques puisque le décret d'application qui décrit les différentes situations susceptibles d'être analysées par le traitement algorithmique peuvent faire apparaître de telles données. De plus, la loi JOP conditionne le recours aux caméras « augmentées » à un simple rôle d'alerte et ne peut donc pas fonder de décision juridique sur son propre avis concernant une situation « anormale » (B).

A. L'absence textuelle de recours aux données biométriques et à la reconnaissance faciale

Le paragraphe IV de l'article 10 de la loi JOP dispose clairement que : « Les traitements mentionnés au I du présent article n'utilisent aucun système d'identification biométrique, ne traitent aucune donnée biométrique et ne mettent en œuvre aucune technique de reconnaissance faciale ». Ces interdictions correspondent aux définitions établies par la CNIL permettant de distinguer les caméras « augmentées » et les caméras biométriques⁶⁷. Toutefois, la loi laisse au pouvoir réglementaire le soin de déterminer les situations anormales que devront détecter les caméras « augmentées » afin de mieux garantir la sécurité des grandes manifestations sportives, récréatives et culturelles susceptibles de faire l'objet d'acte de terrorisme ou d'atteintes graves à la sécurité des personnes. C'est à cette occasion que des interrogations peuvent être soulevées concernant l'absence de traitement de données biométriques.

⁶⁷ Annexe I: *op. cit.*

En effet, l'article 3 du décret du 28 août 2023⁶⁸ désigne les situations anormales que devront détecter les caméras « augmentées », il s'agit de constater : « [la] présence d'objets abandonnés ; [la] présence ou [l'] utilisation d'armes, parmi celles mentionnées à l'article R. 311-2 du code de la sécurité intérieure ; [le] non-respect par une personne ou un véhicule, du sens de circulation commun ; [le] franchissement ou présence d'une personne ou d'un véhicule dans une zone interdite ou sensible ; [la] présence d'une personne au sol à la suite d'une chute ; [un] mouvement de foule ; [une] densité trop importante de personnes ; [des] départs de feux ». Il convient de rappeler que la détection de toutes ces situations anormales peut s'effectuer sur le lieu de l'évènement en question, dans les véhicules et emprises de transport public desservant ce lieu, ainsi que sur le lieu des fan-zones. Ces situations peuvent être classées selon deux catégories. D'une part, il y a les situations anormales qui pourraient être qualifiées de « situationnelles », c'est-à-dire que l'élément central de la situation n'est pas une personne. Par exemple, la détection d'un départ de feux ne requiert pas la présence d'une personne sur les images pour que le traitement algorithmique le détecte. C'est la même logique qui s'applique concernant la présence d'un objet abandonné. Les autres situations anormales qui devront être détectées par les caméras « augmentées » pourraient être qualifiées de « comportementales ». En effet, ces situations requièrent l'analyse du comportement d'une personne par le traitement algorithmique afin de détecter si la situation est anormale ou pas. Tel sera le cas lorsqu'il y a utilisation d'une arme ou un mouvement de foule. Le problème juridique se situe à cet endroit puisque la loi interdit l'analyse des données biométriques des personnes, or les données comportementales sont considérées par le règlement général sur la protection des données⁶⁹ (RGPD) comme des données biométriques « qui permettent ou confirment son identification unique [...] »⁷⁰. Concrètement, pour détecter un mouvement de foule le traitement algorithmique va prendre en compte la vitesse de déplacement des personnes. Bien que le traitement algorithmique ne puisse pas connaître l'identité d'une personne il y a tout de même une opération d'analyse du comportement qui s'opère puisque c'est à

⁶⁸ Décret n° 2023-828 du 28 août 2023 relatif aux modalités de mise en œuvre des traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs, pris en application de l'article 10 de la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions.

⁶⁹ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

⁷⁰ Article 4, §14 du RGPD.

partir de cette analyse du comportement individuel que la situation sera considérée comme anormale par le traitement algorithmique. Il convient donc, sur ce sujet, de rejoindre la position de Céline CASTETS-RENARD et Amélie TURCI lesquelles considèrent que la frontière que tente de construire la loi entre l'analyse du comportement d'une foule et du comportement d'une personne individuelle est « mince »⁷¹, la finalité restant d'appréhender la personne étant à l'origine du mouvement de foule si cela est possible.

Par ailleurs, la loi interdit la reconnaissance faciale dans le recours aux caméras « augmentées ». Cette interdiction est constante en matière de vidéoprotection. Néanmoins, la reconnaissance faciale est utilisée dans divers domaines de l'action publique comme le montre l'étude du Conseil d'État de 2022 à ce sujet⁷². Beaucoup de fantasmes gravitent autour de la reconnaissance faciale d'origine étatique et ceux-ci sont alimentés par les dystopies comme *1984* de George ORWELL ou bien les séries télévisées américaines comme *Person of interest* dont le générique fait état d'une « machine » qui surveille la population en continue⁷³. Ces fantasmes sont également alimentés par l'usage de la reconnaissance faciale en Chine. Cet usage constitue le fondement du système prénommé « crédit social ». Celui-ci va classer les citoyens en catégories avec les bons citoyens et les mauvais citoyens en prenant en compte toutes leurs actions quotidiennes comme aller jeter leurs poubelles⁷⁴.

⁷¹ (C.) CASTETS-RENARD et (A.) TURCI, « 'Caméras augmentées' : un danger pour les libertés lors des Jeux Olympiques et Paralympiques (et au-delà) ? », *Recueil Dalloz*, numéro 22, 2023, p. 2.

⁷² CE, « Intelligence artificielle et action publique : construire la confiance, servir la performance », étude adoptée en assemblée générale plénière du 31 mars 2022.

⁷³ « *You are being watched. The government has a secret system: a machine that spies on you every hour of every day. [...] I designed the Machine to detect acts of terror, but it sees everything. Violent crimes involving ordinary people, people like you. [...] You'll never find us, but victim or perpetrator, if your number's up, we'll find you* », (Lien YouTube: <https://www.youtube.com/watch?v=g6rNf6lvCd4> consulté le 5 novembre 2023).

⁷⁴ CE, « Intelligence artificielle et action publique, *op. cit.*, » : « Certains districts en Chine ont quant à eux opté pour un algorithme de reconnaissance faciale qui identifie la personne se présentant devant une benne à ordures et ouvre le couvercle s'il s'agit d'un résident local. La poubelle contrôle la correspondance entre le sac poubelle jeté et le bac dans lequel il l'est et des points, des crédits ou des bons d'achat, correspondant le cas échéant à la valeur de marché des déchets jetés, peuvent être accordés aux citoyens exemplaires dans le recyclage de leurs déchets », p. 271.

B. La fonction d’alerte des caméras « augmentées »

Cette fonction est prévue au paragraphe IV de l’article 10 de la loi JOP puisque « [les traitements algorithmiques] procèdent exclusivement à un signalement d’attention ». Le législateur surenchérit en ajoutant que cet outil ne peut fonder, « par lui même, aucune décision individuelle ni aucun acte de poursuite ». Enfin, le législateur enterre toute hypothèse de prise d’initiative des traitements algorithmiques puisqu’il précise clairement dans ce paragraphe que les traitements algorithmiques « demeurent en permanence sous le contrôle des personnes chargées de leur mise en oeuvre ». Le législateur a grandement utilisé le champ lexical des restrictions, voire des interdictions, afin d’encadrer et de limiter le plus possible les compétences des futurs traitements algorithmiques. La loi JOP laisse donc la primauté à l’humain et à sa décision comme l’avait préconisé le Conseil d’État dans son avis concernant le projet de loi JOP⁷⁵. Ces limitations relatives à l’emploi des caméras « augmentées » vont dans la bonne direction étant donné les réticences vis-à-vis de la police prédictive mais plus généralement parce que les algorithmiques peuvent contenir des biais de données, des biais de variable oubliée ou des biais de sélection et tous ces biais pourraient constituer des décisions discriminatoires en fonction de l’ethnie ou du sexe de la personne concernée. De plus, la position française en matière d’intelligence artificielle pour la sécurité consiste en ce qu’elle doit rester un outil d’aide à la décision humaine et cela semble être une position équilibrée en démocratie.

Concrètement les traitements algorithmiques qui seront incorporés dans les caméras de vidéoprotection auront pour mission de détecter les événements prédéterminés qui sont inscrits dans le décret d’application de la loi JOP. Une fois une situation anormale détectée sur le lieu d’une manifestation sportive, récréative ou culturelle ou dans une fan-zone ou dans les emprises de transport public une alerte apparaît pour la personne en charge de l’exploitation des caméras. Les personnes pouvant avoir accès aux images et donc aux alertes sont mentionnées au premier paragraphe de l’article 10 de la loi JOP et cette liste comprend: « la police nationale, la gendarmerie nationale, les services d’incendie et de secours, les services de police municipale et les services internes de sécurité de la SNCF et de la Régie autonome des transports parisiens ». Ensuite, il

⁷⁵ CE, avis, n° 406383, relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, p. 7-8.

reviendra à cette personne de confirmer l'alerte et de déclencher les secours adéquats ou bien de mettre un terme à l'alerte si celle-ci s'avère erronée.

La finalité des caméras « augmentées » est avant tout d'aider l'humain dans sa prise de décision en analysant des milliers de personnes en continue en même temps et donc de permettre à l'agent de gagner en efficacité et en réactivité. En effet, l'efficacité des caméras de vidéoprotection dans leur ensemble ne se ressent pas nécessairement sur la baisse de la délinquance mais plutôt sur l'aspect organisationnel de la réponse de la force publique comme le constatent Alain BAUER et François FREYNET dès 2008⁷⁶.

La réalisation de cette étude portant sur le régime juridique de l'expérimentation des caméras « augmentées » a permis de mieux comprendre leur rôle dans la sécurisation des grands événements ainsi que les enjeux relatifs à leur déploiement. Cette étude a également permis de voir que le régime juridique mis en place ne s'inscrit pas dans la lignée de toutes les fictions autour de l'intelligence artificielle et la surveillance de masse des populations. Les caméras « augmentées » sont, pour le moment, un outil d'aide pour les forces de sécurité intérieure et visent à mieux garantir la sécurité dans des lieux accueillant beaucoup de personnes en même temps.

Malgré tout, cette technologie reste attentatoire en ce qui concerne les droits et libertés fondamentaux notamment la protection de la vie privée. Il convient donc désormais de s'intéresser aux garanties inscrites dans la loi JOP mais plus largement aux garanties classiques de protection de la vie privée lorsque l'autorité publique souhaite les restreindre. En effet, malgré le régime expérimental des caméras « augmentées » les garanties classiques de protection des droits et libertés fondamentaux s'appliquent et il convient donc d'étudier la conciliation entre sécurité et liberté dans ce nouveau chapitre.

⁷⁶ (A.) BAUER et (F.) FREYNET, *Vidéosurveillance et vidéoprotection*, Paris, PUF, coll. Que sais-je ?, 2008, p. 34 : « Dans ce cadre, la mesure de l'efficacité de la vidéoprotection n'est pas la baisse de la criminalité constatée, mais le gain organisationnel et la possibilité d'augmenter la présence policière sans multiplier les effectifs ».

Chapitre 2 : Les nécessaires garanties de protection de la vie privée lors du recours des caméras « augmentées »

Le premier chapitre a permis de montrer l'étendue des possibilités pour les pouvoirs publics lorsqu'ils souhaiteraient recourir aux caméras « augmentées ». En effet, selon l'interprétation de l'article 10 de la loi JOP qui sera privilégiée, il sera possible de déployer ces dispositifs sur un périmètre géographique bien plus étendu que celui qui pouvait initialement être imaginé à la simple lecture de la loi.

Désormais, il convient de s'intéresser aux différentes atteintes possibles aux droits et libertés fondamentaux que le déploiement de ces outils sur un large périmètre géographique peut provoquer pour les personnes qui y sont soumises. Ce chapitre sera principalement focalisé sur les diverses atteintes portées au droit au respect de la vie privée, mais il permettra également de voir quelles garanties ont été mises en place. Il convient dans un premier temps de définir et de circonscrire précisément ce que recouvre la notion de droit au respect de la vie privée (section 1). Dans un deuxième temps, il faudra étudier le régime juridique de la police administrative en l'appliquant à l'expérimentation des caméras « augmentées » puisque ces dernières ont pour perspective d'assurer la sécurité de très grands événements, il s'agit donc d'un objectif de prévention des troubles à l'ordre public (section 2).

Section 1 : La définition de la notion de droit au respect de la vie privée

J. RIVERO définissait la vie privée comme : « cette sphère de chaque existence dans laquelle nul ne peut s'immiscer sans y être convié. La liberté de la vie privée est la reconnaissance, au profit de chacun, d'une zone d'activité qui lui est propre et qu'il est maître d'interdire à autrui »⁷⁷. Autrement dit, la vie privée se rattache à l'intimité d'une personne et empêche toute intrusion d'origine étatique ou provenant d'un tiers dans cette sphère personnelle.

Affirmer le principe d'un droit au respect de la vie privée suppose, en outre, qu'il soit protégé tant au niveau du droit national qu'au niveau du droit international (Paragraphe 1). Par ailleurs, le droit au respect de la vie privée est extrêmement vaste puisqu'il peut concerner tous les

⁷⁷ (J.) RIVERO, *Libertés publiques*, Montchrestien, 1989, p. 74.

aspects de la vie d'une personne ainsi que diverses matières juridiques. C'est pour cela que le Conseil constitutionnel a décidé, en 1999, de modifier le fondement constitutionnel du droit au respect de la vie privée en le rattachant désormais à l'article 2 de la Déclaration de 1789 et non plus à l'article 66 de la Constitution de 1958. Ce changement de fondement juridique concernant ce droit a permis de préserver la compétence de la juridiction administrative dans cette matière. C'est cette dernière compétence qui sera étudiée puisque les caméras « augmentées » sont des outils de police administrative et sont une source d'inquiétude concernant le respect du droit à la vie privée (Paragraphe 2).

Paragraphe 1 : La protection composite du droit au respect de la vie privée

Lors de la remise de son rapport au Président de la République intitulé « Redécouvrir le préambule de la Constitution », le comité VEIL a décidé de ne formuler aucune recommandation concernant la constitutionnalisation du droit au respect de la vie privée⁷⁸. En effet, le comité a estimé qu'une telle constitutionnalisation « serait dépourvue de toute portée pratique » puisque, selon lui, ce droit était d'ores et déjà suffisamment protégé en France. D'une part, le législateur est soumis à la jurisprudence du Conseil constitutionnel qui détient sa propre définition du droit au respect de la vie privée (A). D'autre part, il est soumis aux engagements internationaux de la France, lesquels vont offrir une protection supplémentaire au droit au respect de la vie privée (B).

⁷⁸ Comité (S.) VEIL, rapport au Président de la République : « Redécouvrir le Préambule de la Constitution », 17 décembre 2008, p. 70.

A. La jurisprudence du Conseil constitutionnel concernant la protection du droit au respect de la vie privée

Le droit au respect de la vie privée a fait l'objet d'une « irrésistible ascension au sein de la hiérarchie des normes » selon M.-T. MEULDERS-KLEIN⁷⁹. En effet, depuis 1970⁸⁰ ce droit était uniquement protégé à l'article 9 du Code civil qui disposait : « Chacun a droit au respect de sa vie privée ». Cette protection juridique semblait insuffisante puisqu'elle n'avait que valeur législative, il fallait donc accroître le niveau de protection de ce droit au sein de la pyramide des normes. Le Conseil constitutionnel a, pour la première fois, mentionné le droit au respect de la vie privée dans sa décision du 18 janvier 1995 relative à la loi d'orientation et de programmation relative à la sécurité⁸¹, lorsqu'il décidait de la conformité à la Constitution du régime juridique mis en place pour la mise en oeuvre des caméras de vidéosurveillance. Dans cette décision, le droit au respect de la vie privée était fondé sur l'article 66 de la Constitution relatif à la liberté individuelle⁸². Toutefois, le Conseil constitutionnel a considéré qu'un tel fondement ne permettait de protéger le droit au respect de la vie privée dans son ensemble puisque cet article ne concerne que l'autorité judiciaire. Or, les Sages avaient constaté que les autorités publiques pouvaient porter atteinte au droit au respect de la vie privée des individus au-delà des seules mesures pénales. De plus, dans un souci de respecter le principe de la séparation des pouvoirs il fallait modifier le fondement constitutionnel de ce droit pour que la juridiction administrative soit compétente pour traiter ce contentieux. Cela fut chose faite à partir de la décision du 23 juillet 1999⁸³ puisque désormais le droit au respect de la vie privée a pour fondement l'article 2 de la Déclaration de 1789⁸⁴.

⁷⁹ (M.-T.) MEULDERS-KLEIN, « L'irrésistible ascension de la vie privée au sein des droits de l'homme », in *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, dir. (F.) SUDRE, Bruylant, 2005, p.305 s., in (V.) MAZEAUD, « La constitutionnalisation du droit au respect de la vie privée », NCCC n°48 (dossier : vie privée), juin 2015, p. 7 à 20.

⁸⁰ Loi n° 70-643 du 17 juillet 1970 *tendant à renforcer la garantie des droits individuels des citoyens*.

⁸¹ Cons. const., 18 janvier 1995, n° 94-352 DC, *Loi d'orientation et de programmation relative à la sécurité*.

⁸² Article 66 de la Constitution : « Nul ne peut être arbitrairement détenu. / L'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi ».

⁸³ Cons. const., 23 juillet 1999, n° 99-416 DC, *Loi portant création d'une couverture maladie universelle*.

⁸⁴ *Ibid*, considérant 45 : « Considérant qu'aux termes de l'article 2 de la Déclaration des droits de l'homme et du citoyen : « Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression. » ; **que la liberté proclamée par cet article implique le respect de la vie privée** ; ».

Pour déterminer si une loi porte atteinte au droit au respect de la vie privée de manière conforme à la Constitution, le Conseil constitutionnel a dégagé divers principes et objectifs qui s'imposent au législateur. Pour se raccrocher au sujet des caméras « augmentées » et plus largement aux caméras de vidéoprotection classiques, le législateur doit poursuivre l'objectif à valeur constitutionnelle de sauvegarde de l'ordre public, lequel a été créé par la décision du 27 juillet 1982⁸⁵. Il revient donc au législateur d'adopter toutes les mesures nécessaires afin de respecter cet objectif. Par exemple, dans sa décision du 18 janvier 1995⁸⁶ le Conseil constitutionnel a considéré que le régime juridique des caméras de vidéosurveillance était compatible avec cet objectif à valeur constitutionnelle. Pour rendre cette décision, les Sages avaient dû opérer une mise en balance des intérêts entre la sauvegarde de l'ordre public et le droit au respect de la vie privée puisqu'il s'agit de deux normes ayant valeur constitutionnelle, par conséquent aucune norme ne prime sur l'autre. Afin de concilier ces deux normes le juge constitutionnel vérifie que l'atteinte portée au droit au respect de la vie privée soit nécessaire, proportionnée et adaptée. Par exemple, dans sa décision du 17 mai 2023 relative à la loi JOP les Sages considèrent que le dispositif mis en place par le législateur pour la mise en oeuvre des caméras « augmentées » est conforme à la Constitution puisqu'il respecte à la fois l'objectif à valeur constitutionnelle de sauvegarde de l'ordre public et ne porte pas atteinte de manière disproportionnée au droit au respect de la vie privée⁸⁷.

Bien que le droit au respect de la vie privée ne soit pas expressément mentionné dans les textes de valeur constitutionnelle, il est remarquable de constater qu'il fait l'objet d'une protection de la part du Conseil constitutionnel qui s'est renforcée au fil du temps. Le renforcement de la protection de ce droit s'est opéré en parallèle de sa reconnaissance dans les conventions internationales auxquelles la France est partie.

⁸⁵ Cons. const., 27 juillet 1982, n° 82-141 DC, *Loi sur la communication audiovisuelle*, considérant 5 : « Considérant qu'ainsi il appartient au législateur de concilier, [...] d'une part, les contraintes techniques inhérentes aux moyens de la communication audiovisuelle et, d'autre part, les objectifs de valeur constitutionnelle que sont la sauvegarde de l'ordre public, [...] ; ».

⁸⁶ Cons. const., 18 janvier 1995, n° 94-352 DC, *Loi d'orientation et de programmation relative à la sécurité*.

⁸⁷ Cons. const., 17 mai 2023, *op. cit.*, considérant 46 : « Il résulte de ce qui précède, compte tenu des garanties mentionnées ci-dessus et sous la réserve énoncée au paragraphe 39, que les dispositions contestées ne méconnaissent pas le droit au respect de la vie privée ».

B. La protection internationale du droit au respect de la vie privée

Le droit au respect de la vie privée a émergé dans les conventions internationales après la Seconde Guerre mondiale. Ces conventions avaient pour vocation de replacer l'individu au cœur des systèmes juridiques démocratiques. La première convention à faire apparaître le droit au respect de la vie privée est la Déclaration Universelle des Droits de l'Homme de 1948, laquelle prévoit symboliquement dans son article 12 que : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ». Cette diffusion du droit au respect de la vie privée au niveau international va toucher d'autres conventions qui ont des effets contraignants juridiquement. La plus célèbre d'entre elles est la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (Conv.EDH), cette dernière prévoit dans son article 8 §1 que : « 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ». Le droit au respect de la vie privée est également protégé au sein du pacte international relatif aux droits civils et politiques⁸⁸ ainsi que dans la charte des droits fondamentaux de l'Union européenne⁸⁹.

Malgré ces différents articles, il est possible de dégager un régime juridique général relatif à la protection du droit au respect de la vie privée. Ce régime juridique sera surtout focalisé sur la Conv.EDH puisque la Cour Européenne des Droits de l'Homme (CEDH) est celle qui connaît le plus de contentieux avec 160 violations de l'article 8 de la Conv.EDH en 2023⁹⁰. Tout d'abord, ces différents articles insistent sur le fait que ce droit concerne « toute personne ». Dès lors, il ne suppose aucune considération tenant à la nationalité des personnes en cause du moment qu'elles tombent sous la juridiction de l'Etat qui est accusé de l'avoir violé. Par ailleurs, tous ces articles énoncent des restrictions, parfois implicites, à la protection de ce droit. En effet, les seules atteintes mises en cause dans ces articles sont celles qui sont arbitraires ou illégales. Autrement dit, lorsque

⁸⁸ Article 17 du Pacte International relatif aux Droits Civils et Politiques : « 1. Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation. / 2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ».

⁸⁹ Article 7 de la charte des droits fondamentaux de l'Union européenne : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications ».

⁹⁰ Statistique issue du tableau « Violation par article et par Etat 2023 » de la Cour.EDH.

les atteintes au droit au respect de la vie privée sont légalement justifiées, il ne pourra pas être invoqué comme ayant été violé. C'est ce que prévoit le §2 de l'article 8 de la Conv.EDH : « 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, [...], à la défense de l'ordre et à la prévention des infractions pénales, [...], ou à la protection des droits et libertés d'autrui ». En d'autres termes, d'un point de vue juridique le droit au respect de la vie privée n'est pas une norme de *jus cogens*, il est donc possible d'y déroger comme cela est expressément prévu dans les conventions internationales. Pour pouvoir déroger à ce droit il faut que la mesure de restriction trouve son fondement sur une base légale, qu'elle soit proportionnée et nécessaire dans une société démocratique c'est-à-dire qu'elle ne soit pas arbitraire.

Le droit au respect de la vie privée est une notion extrêmement large, avec une multitude de juges compétents selon le domaine de la vie privée en cause. Par exemple, le juge pénal est compétent pour contrôler la légalité des actes d'enquête telle que la perquisition et de mesure privative de liberté. A l'inverse, le juge administratif est compétent pour garantir une conciliation adéquate entre le droit au respect de la vie privée est le maintien de l'ordre public. Ce juge va donc s'intéresser aux restrictions concernant ce droit qui prennent racines avant qu'une infraction pénale ne soit commise. C'est le contentieux de ce dernier qui va être au centre de la prochaine partie puisqu'il convient d'appliquer certains composants de ce droit par rapport au déploiement des caméras « augmentées » étant donné l'effet qu'elles peuvent provoquer sur celui-ci comme l'avait remarqué la CNIL⁹¹.

⁹¹ CNIL, position sur les conditions de déploiement des caméras dites « intelligentes » ou « augmentées » dans les espaces publics, juillet 2022.

Paragraphe 2 : L'application du droit au respect de la vie privée aux caméras intelligentes

Après l'étude générale de la notion du droit au respect de la vie privée, il convient de l'appliquer à l'expérimentation des caméras « augmentées » puisque celle-ci comporte des « enjeux nouveaux et substantiels » dans cette matière comme le souligne le Conseil d'État⁹².

Depuis la mise en oeuvre des caméras de surveillance en 1995 la question concernant la protection du droit au respect de la vie privée est au coeur des débats. Les arguments qui sont opposés à la mise en oeuvre de ces caméras, et plus encore opposés aux caméras « augmentées », sont identiques et reposent en premier lieu sur la question du droit à l'anonymat sur la voie publique (A). Par ailleurs, l'expérimentation des caméras « augmentées » apportent des garanties renforcées à des composants numériques du droit au respect de la vie privée tels que le droit d'opposition et le droit d'information (B).

A. Le respect du droit à l'anonymat des personnes soumises aux caméras « augmentées »

Le 26 novembre 2021 la CNIL mettait en demeure la société Clearview AI de se conformer au RGPD afin de, notamment, mieux respecter le droit à l'anonymat. Cette décision a été perçue comme la réaffirmation des « frontières démocratiques de la société numérique »⁹³. Cette société était soupçonnée d'effectuer des traitements de données à caractère personnel sans base légale ainsi que de ne pas suffisamment tenir compte des droits des personnes tel que le droit à l'anonymat puisque les données collectées servaient à alimenter les bases de données d'une surveillance étatique ou privée. Les personnes dont les données étaient exploitées ne pouvaient pas y accéder ni demander leur effacement ce qui portait atteinte à leur droit au respect de la vie privée. Finalement, sans réponse de la part de la société Clearview AI, la CNIL a prononcé une amende de 20 millions

⁹² CE, 15 décembre 2022, avis n° 406383, *op. cit.*, §27, p. 9.

⁹³ (C.) LEQUESNE ROTH, « Mise en demeure de Clearview AI par la CNIL : les jalons d'un combat pour le droit à l'anonymat », *Dalloz*, IP/IT 2022. 220.

d'euros à son encontre⁹⁴. Cette affaire est le symbole d'une époque où le droit à l'anonymat disparaît toujours davantage au profit des nouvelles technologies d'identification des personnes et à l'exploitation de leurs données. La protection du droit à l'anonymat devient donc un enjeu majeur en terme de sécurité publique utilisant des nouvelles technologies. Il n'existe aucune définition légale ou jurisprudentielle de ce que recouvre le droit à l'anonymat dans l'espace public. Mais faisant partie du droit au respect de la vie privée⁹⁵, il s'agirait d'un droit mêlant « secret et liberté »⁹⁶. La Cour.EDH considère qu'est protégée par l'article 8 de la Conv.EDH : « une zone d'interaction entre l'individu et autrui qui, même dans un contexte public, peut relever de la « vie privée »⁹⁷.

Il est sans doute paradoxal de vouloir protéger un tel droit dans l'espace public alors que dans cette matière l'anonymat est par principe interdit puisque la loi du 11 octobre 2010 proscrit formellement la dissimulation du visage⁹⁸. Néanmoins, depuis la mise en oeuvre des caméras sur la voie publique en 1995 le législateur a toujours fait en sorte de protéger ce droit étant donné les importantes atteintes à la vie privée auxquelles elles peuvent conduire notamment au travers du recours à la reconnaissance faciale. C'est la raison pour laquelle la reconnaissance faciale reste interdite en France même pour l'usage des caméras « augmentées ». En effet, cette technologie permet l'identification d'une personne avec un jeu de données à caractère personnel (nom, prénom, âge...), elle analyserait donc toutes les personnes se trouvant dans le champ de vision de la caméra. L'atteinte aux droits et libertés fondamentaux serait disproportionnée dans une démocratie où la liberté prime et donc un droit minimal à l'anonymat doit pouvoir être conservé et protégé même dans l'espace public. A l'inverse, en Chine la reconnaissance faciale est utilisée de manière très

⁹⁴ Site de la CNIL Affaire Clearview AI : <https://www.cnil.fr/fr/reconnaissance-faciale-sanction-de-20-millions-deuros-lencontre-de-clearview-ai> (consulté le 09 avril 2024).

⁹⁵ Cons. const., 18 janvier 1995, n° 94-352 DC, *op. cit.*, considérant 2 : « Considérant que les auteurs des saisines font grief à cet article, qui fixe un régime d'autorisation et d'utilisation des installations de systèmes de vidéosurveillance, de méconnaître l'exercice de plusieurs libertés et droits fondamentaux constitutionnellement protégés ; qu'au nombre de ceux-ci figureraient, selon eux, la liberté individuelle dont l'autorité judiciaire doit assurer la garantie en vertu de l'article 66 de la Constitution, la liberté d'aller et venir sans surveillance arbitraire et généralisée et **le droit au respect de la vie privée qui impliquerait un droit à l'anonymat** ; [...] ».

⁹⁶ (L.) FAVOREU, (A.) DUFFY-MEUNIER, (I.) FASSASSI, (P.) GAÏA, (O.) LE BOT, (L.) PECH, (A.) PENA, (A.) ROUX & (G.) SCOFFONI, *Droit des libertés fondamentales*, Dalloz, coll. Précis, 8e édition, 2021, §267, p. 362.

⁹⁷ CEDH, *Peck c. Royaume-Uni*, n° 44647/ 98, § 57, 28 janvier 2003.

⁹⁸ Loi n° 2010-1192 du 11 octobre 2010 *interdisant la dissimulation du visage dans l'espace public*.

conséquente comme le montre le documentaire « Ma femme a du crédit » où toute la vie quotidienne des chinois est régie par l'image et son utilisation.

Le débat sur la protection du droit à l'anonymat n'a pas pu être de nouveau soulevé lors de l'adoption de la loi JOP puisque son article 10 interdit explicitement le recours à la reconnaissance faciale ainsi qu'à l'exploitation des données biométriques. Autrement dit, les caméras « augmentées » ne peuvent toujours pas identifier de manière unique une personne et cela permet de garantir « la préservation de l'anonymat dans l'espace public, donc l'absence d'atteinte au droit à la vie privée, et les garanties prévues garantissent la neutralité de l'outil »⁹⁹.

En définitive, comme les caméras « augmentées » ne permettent pas d'identifier de manière unique les personnes se trouvant dans leur champ de vision sur la voie publique, le droit à l'anonymat dans l'espace public se trouve ainsi protégé. Les caméras « augmentées » sont des outils de sécurité portant davantage atteinte au droit au respect de la vie privée en conséquence les garanties entourant ces outils doivent être renforcées. C'est pour cela que la loi JOP prévoit de nouvelles garanties pour le droit au respect de la vie privée dans le domaine du numérique.

⁹⁹ CE, étude d'impact sur le projet de loi JOP, 20 décembre 2022, p. 85.

B. Les composants numériques du droit au respect de la vie privée soumis aux caméras « augmentées »

Les caméras « augmentées » sont soumises au RGPD comme l'indique clairement le paragraphe II de l'article 10 de la loi JOP. Dès lors, les données collectées par celles-ci doivent être traitées de manière conforme à ce règlement afin de pouvoir respecter le droit au respect de la vie privée.

L'une des problématiques soulevées concernant le recours aux caméras « augmentées » concerne le droit d'opposition. Ce droit est défini à l'article 21 du RGPD¹⁰⁰ et permet à toute personne, à tout moment, de s'opposer au traitement de ses données par le responsable du traitement. Pour manifester son opposition relativement au traitement de ses données il est possible d'appuyer « sur un bouton, [de faire] un geste particulier devant une caméra ou [de stationner] dans une zone dédiée »¹⁰¹. Il est à noter que les caméras « augmentées » font partie des traitements de données mentionnés au point (e) du paragraphe 1 de cet article puisqu'elles ont pour intention de mieux garantir la sécurité des manifestations sportives, récréatives et culturelles, il s'agit par conséquent de l'exercice de l'autorité publique. Le droit d'opposition pourrait donc s'appliquer vis-à-vis de ces caméras. Néanmoins, le paragraphe 1 de l'article 21 du RGPD prévoit qu'il est possible de limiter le droit d'opposition s'il est démontré qu'il « existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée ».

¹⁰⁰ Article 21 du RGPD : « 1. La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur l'article 6, paragraphe 1, point e) ou f), y compris un profilage fondé sur ces dispositions. Le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice. / 2. Lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée a le droit de s'opposer à tout moment au traitement des données à caractère personnel la concernant à de telles fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection. / 3. Lorsque la personne concernée s'oppose au traitement à des fins de prospection, les données à caractère personnel ne sont plus traitées à ces fins ».

¹⁰¹ (L.) FAUVEL, (S.) REVOL et (M.-E.) HURNIC, « 'Caméras « intelligentes » : sécuriser leur conformité au RGPD », *Revue Lamy Droit de l'Immatériel*, No 200, 1er février 2023, p. 2.

De plus, le droit d'opposition peut être proscrit par « une mesure législative »¹⁰² pour certains types de traitement de données comme le prévoit l'article 23 du RGPD. En l'espèce, le décret n° 2023-828 du 28 août 2023 prévoit que le droit d'opposition ne s'applique pas aux traitements algorithmiques des images collectées par les caméras « augmentées »¹⁰³. L'interdiction de recourir au droit d'opposition dans le contexte des caméras « augmentées » vise à protéger l'objectif poursuivi par celles-ci qui est d'assurer la sécurité des manifestations sportives, récréatives et culturelles tout en détectant des situations anormales. En effet, l'exercice d'un tel droit aurait été « antinomique »¹⁰⁴ par rapport à la mission à atteindre.

Bien que l'exercice du droit d'opposition soit proscrit dans le domaine des caméras « augmentées », il faut assurer un minimum de protection pour les personnes concernées par ces traitements algorithmiques et cela va intervenir au travers d'une information renforcée concernant leur présence. Le droit d'information relatif à la présence d'une caméra de vidéoprotection dans l'espace public est une obligation depuis 1995¹⁰⁵ et celui-ci a été renforcé par la loi JOP¹⁰⁶. L'information « est délivrée par tout moyen approprié »¹⁰⁷ comme par exemple au travers de la présence d'un panneau¹⁰⁸ sur lequel sera précisé différents éléments, ou bien au travers d'affiches

¹⁰² La notion de « mesure législative » doit se comprendre conformément au considérant 41 du RGPD : « Lorsque le présent règlement fait référence à une base juridique ou à une mesure législative, cela ne signifie pas nécessairement que l'adoption d'un acte législatif par un parlement est exigée, sans préjudice des obligations prévues en vertu de l'ordre constitutionnel de l'État membre concerné. Cependant, cette base juridique ou cette mesure législative devrait être claire et précise et son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour de justice de l'Union européenne (ci-après dénommée « Cour de justice ») et de la Cour européenne des droits de l'homme ».

¹⁰³ Décret n° 2023-828, 28 août 2023, *op.cit.*, article 10.

¹⁰⁴ (A.) EGEA, (L.) TAÏEB, (B.) PELLAN et (G.) GOLDBERG, « Actualité Informatique et libertés », Dalloz, *AJDA*, n° 9/2023, 13 mars 2023, p. 3.

¹⁰⁵ Article 10 de la loi du 21 janvier 1995, n° 95-73 : « Le public est informé de manière claire et permanente de l'existence du système de vidéoprotection et de l'autorité ou de la personne responsable ».

¹⁰⁶ Article 10, § III de la loi JOP : « III. – Le public est préalablement informé, par tout moyen approprié, de l'emploi de traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection autorisés sur le fondement de l'article L. 252-1 du code de la sécurité intérieure et de caméras installées sur des aéronefs autorisés sur le fondement du chapitre II du titre IV du livre II du même code, sauf lorsque les circonstances l'interdisent ou que cette information entrerait en contradiction avec les objectifs poursuivis ».

¹⁰⁷ Décret n° 2023-828 du 28 août 2023, *op. cit.*, article 17.

¹⁰⁸ Annexe IV : Panneaux d'information de la présence de caméras de vidéoprotection produits par la CNIL.

dédiées spécifiquement à informer le public de la présence de caméras « augmentées »¹⁰⁹. En effet, doivent être mentionnés la base légale du traitement, les destinataires des données personnelles et des informations complémentaires si besoin¹¹⁰. Par ailleurs, le paragraphe III de l'article 10 de la loi JOP prévoit la possibilité de ne pas informer le public sur la présence de caméras « augmentées » si « les circonstances l'interdisent ou que cette information entrerait en contradiction avec les objectifs poursuivis ». Néanmoins, cette hypothèse est traitée de manière très délicate par la CNIL qui a rappelé fin 2022 que « [L]a mise en œuvre [du droit d'information] est indispensable pour permettre le déploiement de dispositifs de caméras augmentées dans un climat de confiance à l'égard des autorités publiques »¹¹¹. Dès lors, les hypothèses où serait écarté un tel droit doivent être particulièrement précises et réduites selon la CNIL. De même, une interdiction totale de cette information ne doit être que la seule solution possible pour assurer la sécurité de telle manifestation mais lorsqu'une information même partielle sur la présence des caméras « augmentées » peut être mise en oeuvre il faudra qu'elle le soit pour assurer ce climat de confiance entre les personnes et les autorités publiques.

L'autorisation de recourir aux caméras « augmentées » pour assurer la sécurité des manifestations sportives, récréatives et culturelles peut présenter des risques concernant la protection des droits et libertés fondamentaux, notamment le droit au respect de la vie privée. Toutefois, le régime juridique mis en place semble assez équilibré et permet de concilier les impératifs de sécurité tout en protégeant les différents aspects du droit au respect de la vie privée des personnes qui seront soumises à ces dispositifs. Le succès de la mise en oeuvre des caméras « augmentées » repose en grande partie sur le respect, par les autorités publiques, du droit à l'information du public afin d'instaurer ce climat de confiance qui est très important en matière d'usage des nouvelles technologies pour la sécurité publique.

Malgré ces diverses obligations s'imposant aux autorités publiques pour protéger les droits et libertés fondamentaux des personnes, d'autres mécanismes vont permettre aux personnes de faire

¹⁰⁹ Arrêté, n° 2024-00493, de la préfecture de police autorisant le recours aux caméras « augmentées » dans deux gares parisiennes afin de sécuriser le match de Football PSG-OL, 17 avril 2024. Il précise que l'information au public de la présence de ces dispositifs se fera au travers de « 31 affiches » ainsi que de QR code.

¹¹⁰ Site de la CNIL : <https://www.cnil.fr/fr/la-videosurveillance-videoprotection-sur-la-voie-publique> (consulté le 13 avril 2024).

¹¹¹ CNIL, délibération n° 2022-118 du 8 décembre 2022.

respecter leurs droits. En effet, les caméras « augmentées » sont un dispositif de police administrative ce qui signifie qu'il pourra être contesté devant le juge administratif.

Section 2 : La vidéoprotection intelligente, un outil de police administrative

Selon Alain BAUER et François FREYNET le passage à l'acte délinquant suppose trois éléments cumulatifs : la motivation, la facilité et l'anonymat. Si l'un de ces trois éléments disparaît le passage à l'acte peut être évité, selon le type de délinquant. Pour ces auteurs les caméras de vidéoprotection vont agir sur l'anonymat puisque elles vont permettre d'identifier *a posteriori* les individus et vont également affecter la facilité, c'est-à-dire le lieu de commission de l'infraction, dans un aspect de prévention des troubles à l'ordre public¹¹². Dans cette perspective, les caméras de vidéoprotection sont des outils de police administrative et ce régime va également s'appliquer aux caméras « augmentées » puisqu'elles visent à garantir l'ordre public lors des manifestations sportives, récréatives et culturelles.

La loi JOP prévoit un régime juridique de droit administratif pour l'usage des caméras « augmentées », celles-ci supposent une autorisation préfectorale (Paragraphe 1). Par ailleurs, la contestation relative à leur recours peut se faire devant le juge administratif (Paragraphe 2).

¹¹² (A.) BAUER et (F.) FREYNET, *Vidéosurveillance et vidéoprotection*, Paris, PUF, coll. Que sais-je ?, 2008, p. 35.

Paragraphe 1 : Le nécessaire arrêté préfectoral autorisant le déploiement des caméras « augmentées »

Une autorisation préfectorale est nécessaire pour la mise en oeuvre d'une caméra de vidéoprotection qu'elle soit classique¹¹³ ou « intelligente »¹¹⁴. Cette autorisation préfectorale est soumise à plusieurs conditions définies aux articles L.252-1 et suivants du code de la sécurité intérieure mais également par le paragraphe VII de l'article 10 de la loi JOP¹¹⁵. Cette autorisation doit être extrêmement précise¹¹⁶ concernant les finalités pour lesquelles une caméra de vidéoprotection est mise en oeuvre mais également le délai pendant lequel sont conservées les images collectées, délai ne pouvant dépasser un mois¹¹⁷.

Concernant les caméras « augmentées », elles ont pour dessein de lutter contre le haut du spectre dans les atteintes à l'ordre public et cela les empêche donc d'être déployées pour prévenir les seules atteintes aux biens¹¹⁸. Ces caméras seront donc mises en oeuvre afin de lutter contre les atteintes physiques les plus graves pour les personnes et prévenir tout acte de terrorisme. Toutefois, l'autorisation préfectorale doit justifier de l'existence concrète d'un tel risque pour que l'usage des caméras « augmentées » soit proportionné et ne peut pas simplement les évoquer de manière

¹¹³ Article L.252-1 du CSI: « L'installation d'un système de vidéoprotection dans le cadre du présent titre est subordonnée à une autorisation du représentant de l'Etat dans le département et, à Paris, du préfet de police [...] ».

¹¹⁴ Article 10, § VII de la loi JOP : « L'emploi du traitement est autorisé par le représentant de l'Etat dans le département ou, à Paris, par le préfet de police. Cette autorisation peut être accordée uniquement lorsque le recours au traitement est proportionné à la finalité poursuivie ».

¹¹⁵ Article 10, § VII loi JOP : « [...] La décision d'autorisation est motivée et publiée. Elle précise :

1° Le responsable du traitement et les services associés à sa mise en oeuvre ;

2° La manifestation sportive, récréative ou culturelle concernée et les motifs de la mise en oeuvre du traitement au regard de la finalité mentionnée au I ;

3° Le périmètre géographique concerné par la mise en oeuvre du traitement dans les limites mentionnées au même I ;

4° Les modalités d'information du public, notamment sur ses droits, ou, lorsque cette information entre en contradiction avec les objectifs poursuivis, les motifs pour lesquels le responsable du traitement en est dispensé, accompagnés d'un renvoi vers l'information générale organisée par le ministère de l'intérieur mentionnée au second alinéa du III ;

5° La durée de l'autorisation. Cette durée ne peut excéder un mois et est renouvelable selon les modalités prévues au présent VII lorsque les conditions de la délivrance de l'autorisation demeurent réunies ».

¹¹⁶ Annexe V : Exemple d'autorisation préfectorale de déploiement de caméras de vidéoprotection sur Paris (06e) en date du 19 février 2018, n° 20180136.

¹¹⁷ Article L.252-5 CSI.

¹¹⁸ Cons. const., 17 mai 2023, *op. cit.*,

abstraite (A). Par ailleurs, le Conseil constitutionnel a limité la durée de l'autorisation de recourir aux caméras « augmentées » à la seule durée de l'évènement qu'il convient de sécuriser (B).

A. L'insuffisante référence générale à la lutte antiterroriste pour justifier l'utilisation des caméras « augmentées »

Depuis la loi du 21 janvier 1995 la vidéosurveillance - depuis 2011 la vidéoprotection - constitue « un moyen de renforcer la sécurité de la voie publique et des lieux ouverts au public »¹¹⁹. Au fil du temps, les critères permettant de justifier le déploiement de ces caméras se sont étoffés. En effet, la loi de 1995 ne prévoyait que cinq critères matériels de mise en oeuvre des caméras de vidéoprotection¹²⁰. Il fallait attendre la loi du 23 janvier 2006¹²¹ pour que « la prévention d'actes de terrorisme » puisse être un nouveau critère de mise en oeuvre des caméras de vidéoprotection. Cette loi de 2006 s'inscrivant par nature dans le contexte terroriste de l'époque avec les attentats commis à Madrid en 2004 et à Londres en 2005. Par ailleurs, le déploiement des caméras de vidéoprotection à la fin de lutter contre le terrorisme fait l'objet d'un régime juridique spécifique aux articles L.223-1 et suivants du CSI.

¹¹⁹ Annexe I, loi n° 95-73 du 21 janvier 1995 *d'orientation et de programmation relative à la sécurité*.

¹²⁰ Article 10, de la loi du 21 janvier 1995 LOPS: « [...] II. - *La transmission et l'enregistrement d'images prises sur la voie publique, par le moyen de la vidéosurveillance, peuvent être mis en oeuvre par les autorités publiques compétentes aux fins d'assurer la protection des bâtiments et installations publics et de leurs abords, la sauvegarde des installations utiles à la défense nationale, la régulation du trafic routier, la constatation des infractions aux règles de la circulation ou la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression ou de vol [...] ».*

¹²¹ Loi n° 2006-64 du 23 janvier 2006 *relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*.

En tout état de cause, tous les critères de mise en oeuvre des caméras de vidéoprotection sont mentionnés à l'article L.251-2 du CSI¹²².

La lutte antiterroriste est donc le critère matériel commun pour déployer les caméras de vidéoprotection classiques et les caméras « augmentées ». Pour autoriser le déploiement de ces deux types d'outils, le préfet doit adopter deux arrêtés préfectoraux d'autorisation distincts puisque le traitement algorithmique n'est pas une simple adjonction à une caméra de vidéoprotection classique mais bien un changement de nature de celle-ci. Toutefois, la seule référence générale à la lutte contre le terrorisme ne va pas permettre au préfet d'autoriser le déploiement des caméras « augmentées ». Autrement dit, même si l'ensemble de la France est soumis à un risque élevé d'acte de terrorisme et que le niveau « Urgence Attentat »¹²³ du plan Vigipirate a de nouveau été déclenché, ce seul argument ne sera pas suffisant pour justifier l'autorisation de recourir aux caméras « augmentées ». En effet, pour que l'autorisation de mise en oeuvre des caméras « augmentées » soit légale il faut qu'elle repose sur des besoins particuliers et qu'elle vise à prévenir des risques réels de troubles à l'ordre public ou d'atteinte à l'intégrité physique des personnes.

¹²² Article L.251-2 du CSI: « Des systèmes de vidéoprotection peuvent être mis en œuvre sur la voie publique par les autorités publiques compétentes aux fins d'assurer :

1° La protection des bâtiments et installations publics et de leurs abords ;

2° La sauvegarde des installations utiles à la défense nationale ;

3° La régulation des flux de transport ;

4° La constatation des infractions aux règles de la circulation ;

5° La prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants ainsi que la prévention, dans des zones particulièrement exposées à ces infractions, des fraudes douanières prévues par le dernier alinéa de l'article 414 du code des douanes et des délits prévus à l'article 415 du même code portant sur des fonds provenant de ces mêmes infractions ;

6° La prévention d'actes de terrorisme, dans les conditions prévues au chapitre III du titre II du présent livre ;

7° La prévention des risques naturels ou technologiques ;

8° Le secours aux personnes et la défense contre l'incendie ;

9° La sécurité des installations accueillant du public dans les parcs d'attraction ;

10° Le respect de l'obligation d'être couvert, pour faire circuler un véhicule terrestre à moteur, par une assurance garantissant la responsabilité civile ;

11° La prévention et la constatation des infractions relatives à l'abandon d'ordures, de déchets, de matériaux ou d'autres objets.

Des systèmes de vidéoprotection peuvent également être mis en œuvre dans des lieux et établissements ouverts au public aux fins d'y assurer la sécurité des personnes et des biens lorsque ces lieux et établissements sont particulièrement exposés à des risques d'agression ou de vol.

Après information du maire de la commune concernée et autorisation des autorités publiques compétentes, des commerçants peuvent mettre en œuvre sur la voie publique un système de vidéoprotection aux fins d'assurer la protection des abords immédiats de leurs bâtiments et installations, dans les lieux particulièrement exposés à des risques d'agression ou de vol. Les conditions de mise en œuvre et le type de bâtiments et installations concernés sont définis par décret en Conseil d'Etat ».

¹²³ Le Premier ministre Gabriel Attal a relevé le plan Vigipirate à son niveau le plus élevé « Urgence Attentat » le 24 mars 2024 à la suite des attentats survenus à Moscou.

Concrètement, cette hypothèse est déjà apparue pendant la période d'état d'urgence de 2015 puisqu'à ce moment-là un procureur de la République avait autorisé des opérations de contrôle d'identité de police administrative en tout temps. Cette autorisation a été censurée par la Cour de cassation qui a considéré « qu'en toute hypothèse, la référence au plan Vigipirate et à l'état d'urgence ne permet pas à elle seule de justifier la régularité d'un contrôle d'identité de police administrative, en l'absence de circonstances particulières à l'espèce constitutives d'un risque d'atteinte à l'ordre public »¹²⁴. De même, le Conseil constitutionnel a considéré que : « la pratique de ces opérations de manière généralisée et discrétionnaire serait incompatible avec [...] le droit au respect de la vie privée »¹²⁵. Autrement dit, il faut que le risque d'acte de terrorisme soit avéré à un endroit précis pour qu'une restriction des droits et libertés fondamentaux soit justifiée et proportionnée.

Le raisonnement doit donc être similaire pour le préfet lorsqu'il devra autoriser le déploiement des caméras « augmentées » lors des JOP 24. Pendant cette période, la tentation sera sans doute forte du côté des autorités de police administrative d'autoriser tous les moyens de sécurité afin de prévenir tout trouble à l'ordre public puisqu'il s'agira d'un évènement regroupant des millions de personnes avec de forts risques latents d'acte de terrorisme. Néanmoins, le déploiement des caméras « augmentées » ne sera légal que lorsque l'autorisation préfectorale respectera les trois critères classiques d'un acte de police administrative que sont : la proportionnalité, la nécessité et l'adaptabilité, et qu'un risque réel de trouble à l'ordre public sera caractérisé.

En définitive, ce qui va caractériser l'autorisation de déploiement des caméras « augmentées » ce sont les éléments concrets qui vont justifier celle-ci et non pas simplement son objectif de lutter contre le terrorisme et les atteintes graves à la sécurité des personnes. Par ailleurs,

¹²⁴ Cass, Civ 1^{ère}, 13 septembre 2017, 16-22.967, Publié au bulletin.

¹²⁵ Cons. const., n° 2017-677 QPC, 1er décembre 2017, considérant 6 : « Toutefois, il peut être procédé à ces opérations, dans les lieux désignés par la décision du préfet, à l'encontre de toute personne, quel que soit son comportement et sans son consentement. S'il est loisible au législateur de prévoir que les opérations mises en œuvre dans ce cadre peuvent ne pas être liées au comportement de la personne, la pratique de ces opérations de manière généralisée et discrétionnaire serait incompatible avec la liberté d'aller et de venir et le droit au respect de la vie privée. Or, en prévoyant que ces opérations peuvent être autorisées en tout lieu dans les zones où s'applique l'état d'urgence, le législateur a permis leur mise en œuvre sans que celles-ci soient nécessairement justifiées par des circonstances particulières établissant le risque d'atteinte à l'ordre public dans les lieux en cause ».

cette autorisation est étroitement encadrée dans le temps puisqu'elle est limitée à la durée de l'évènement qu'elle a pour objectif de sécuriser.

B. Le recours aux caméras « augmentées » limité à la durée de l'évènement à sécuriser

« La liberté est la règle, la restriction de police l'exception »¹²⁶. Cette expression irrigue tout le droit de la police administrative puisque c'est sur ce fondement intellectuel qu'il convient de déterminer si un acte de police administrative est proportionné par rapport au maintien de l'ordre public et à l'atteinte qu'il procure aux droits et libertés fondamentaux.

Concrètement pour les caméras « augmentées », la loi JOP prévoit que l'autorisation d'y recourir peut durer un mois maximum et être renouvelée si les conditions pour cela sont toujours réunies¹²⁷. A l'inverse, le paragraphe VIII de l'article 10 de cette loi octroie au préfet le pouvoir de retirer à tout moment cette autorisation s'il apparaît que les conditions de son autorisation ne sont plus réunies. L'intention poursuivie concernant cette autorisation vise à concilier la protection du droit au respect de la vie privée et l'objectif à valeur constitutionnelle de sauvegarde de l'ordre public. Cela est d'autant plus juste que le Conseil constitutionnel a interprété la dernière phrase du paragraphe VIII de l'article 10 de la loi JOP¹²⁸ comme une obligation incombant au préfet de retirer l'autorisation de déploiement des caméras « augmentées » lorsque les conditions ayant justifier celle-ci ne sont plus réunies¹²⁹. Autrement dit, le préfet a l'obligation de retirer sans délai l'autorisation de leur mise en oeuvre lorsque leur recours n'est plus légal et porte donc atteinte de manière disproportionnée au droit au respect de la vie privée des personnes qui y sont soumises.

¹²⁶ Concl. Corneille sur CE 17 août 1917, *Baldy*.

¹²⁷ Article 10, § VII, 5° : « La durée de l'autorisation. Cette durée ne peut excéder un mois et est renouvelable selon les modalités prévues au présent VII lorsque les conditions de la délivrance de l'autorisation demeurent réunies ».

¹²⁸ Paragraphe VIII de l'article 10 de la loi JOP : « [...] / Il peut suspendre l'autorisation ou y mettre fin à tout moment s'il constate que les conditions ayant justifié sa délivrance ne sont plus réunies ».

¹²⁹ Cons. const., 17 mai 2023, *op. cit.*, considérant 39 : « D'autre part, la durée de l'autorisation, qui doit en tout état de cause être proportionnée à celle de la manifestation dont il s'agit d'assurer la sécurité, ne peut excéder un mois et ne peut être renouvelée que si les conditions de sa délivrance continuent d'être réunies. À ce titre, si les dispositions contestées prévoient que le préfet ayant autorisé la mesure « peut suspendre l'autorisation ou y mettre fin à tout moment s'il constate que les conditions ayant justifié sa délivrance ne sont plus réunies », **elles ne sauraient, sans méconnaître le droit au respect de la vie privée, être interprétées autrement que comme obligeant le préfet à mettre fin immédiatement à une autorisation dont les conditions ayant justifié la délivrance ne sont plus réunies** ».

Par ailleurs, dans le même considérant le Conseil constitutionnel a inséré une autre forme de délai concernant l'autorisation du recours aux caméras « augmentées ». Il a précisé que : « la durée de l'autorisation, [...] doit en tout état de cause être proportionnée à celle de la manifestation dont il s'agit d'assurer la sécurité ». Les JOP 24 sont une très grande manifestation sportive, récréative et culturelle mais ils sont découpés en plusieurs petits événements sur la période. En conséquence, ils n'ont pas tous vocation à faire l'objet d'une autorisation de recourir aux caméras « augmentées », puisque celle-ci suppose que des menaces réelles pèsent sur une manifestation en particulier. Cela signifie donc que le préfet va devoir octroyer une autorisation préfectorale pour chaque épreuve des JOP et non pas simplement une seule autorisation pour toute la période des JOP afin que le recours aux caméras « augmentées » soit légal.

Paragraphe 2 : La garantie de l'accès au juge pour contester l'utilisation des caméras « augmentées »

En tant qu'acte administratif unilatéral, l'autorisation préfectorale de recourir aux caméras « augmentées » pour sécuriser les manifestations sportives, récréatives et culturelles doit respecter différents critères pour ne pas affecter de manière disproportionnée les droits et libertés fondamentaux. En cas de contestation de cet acte c'est le juge administratif qui devra déterminer si l'acte est légal ou illégal. Pour cela, les justiciables pourront saisir le juge administratif en référé ou bien lors d'un recours pour excès de pouvoir (A). Par ailleurs, le contentieux concernant le recours à de l'intelligence artificielle dans les caméras de vidéoprotection arrivent devant le juge administratif comme l'illustrent les différentes décisions relatives au logiciel Briefcam (B).

A. Les différents recours possibles devant le juge administratif contre l'usage des caméras « augmentées »

L'autorisation préfectorale concernant l'usage des caméras « augmentées » afin de sécuriser les manifestations sportives, récréatives ou culturelles peut faire l'objet de recours contentieux conformément au premier alinéa l'article R.421-1 du code de justice administrative¹³⁰ (CJA) puisqu'il s'agit d'une décision au sens de cet article. Cette décision peut être attaquée sur le fondement de deux recours contentieux qui sont, d'une part, le référé-liberté et, d'autre part, le recours en excès de pouvoir.

Tout d'abord, le référé-liberté a été introduit par la loi du 30 juin 2000¹³¹ à l'article L.521-2 du CJA¹³². Ce recours permet au juge de prendre toutes les mesures nécessaires afin de garantir la protection d'une liberté fondamentale face à une décision illégale de l'Administration notamment en matière de police administrative. Pour cela, le référé-liberté suppose diverses conditions cumulatives permettant de statuer dans ce délai de « 48 heures ». En premier lieu, il faut qu'il y ait une situation d'urgence qui peut se manifester par rapport à l'atteinte portée à une liberté fondamentale, cette atteinte devant être particulièrement grave. En deuxième lieu, il faut qu'une liberté fondamentale soit affectée par cette décision. La liberté fondamentale doit s'entendre au sens de l'article L.521-2 du CJA et le référé-liberté pourra s'exercer dans le contentieux des caméras « augmentées » puisque le juge des référés du Conseil d'État a reconnu le respect de la vie privée comme une liberté fondamentale en 2007¹³³. Enfin, il faut que l'atteinte portée à la liberté fondamentale soit manifestement illégale, c'est-à-dire qu'il ne faut aucun doute concernant l'illégalité de la décision comme par exemple lorsqu'il s'agit d'une interdiction pure et simple de l'exercice d'une liberté fondamentale. Ce recours pourra donc être utilisé afin de contester le

¹³⁰ Article R.421-1 CJA : « La juridiction ne peut être saisie que par voie de recours formé contre une décision, et ce, dans les deux mois à partir de la notification ou de la publication de la décision attaquée ».

¹³¹ Loi n° 2000-597 du 30 juin 2000 relative au référé devant les juridictions administratives.

¹³² Article L.521-2 CJA : « Saisi d'une demande en ce sens justifiée par l'urgence, le juge des référés peut ordonner toutes mesures nécessaires à la sauvegarde d'une liberté fondamentale à laquelle une personne morale de droit public ou un organisme de droit privé chargé de la gestion d'un service public aurait porté, dans l'exercice d'un de ses pouvoirs, une atteinte grave et manifestement illégale. Le juge des référés se prononce dans un délai de quarante-huit heures ».

¹³³ CE, ord. référé, 25 octobre 2007, n° 310125 : « Considérant que Mme Y demande au juge des référés du Conseil d'Etat, sur le fondement de l'article L. 521-2 du code de justice administrative, afin de sauvegarder le respect de sa vie privée, lequel constitue une liberté fondamentale au sens de cet article [...] ».

recours aux caméras « augmentées », dès lors que celui-ci apparaîtrait comme manifestement disproportionné par rapport à l'atteinte engendrée pour le droit au respect de la vie privée et le bénéfice procuré pour maintenir l'ordre public.

Par ailleurs, les justiciables pourront également utiliser le recours pour excès de pouvoir afin de contester le recours aux caméras « augmentées ». Ce recours pourra être utilisé en parallèle du référé-suspension prévu à l'article L.521-1 du CJA¹³⁴ puisque le juge pourra suspendre l'exécution de recourir aux caméras « augmentées » le temps qu'il statue sur le fond du recours pour excès de pouvoir. En effet, le recours pour excès de pouvoir offre au juge davantage de pouvoir pour décider de la légalité de la décision notamment en ayant recours à un contrôle de proportionnalité de celle-ci. Le juge va, dans le cadre de ce recours, affiner son contrôle afin de déterminer si l'usage des caméras « augmentées » est proportionné à la sauvegarde de l'ordre public et s'il ne porte pas une atteinte disproportionnée au droit au respect de la vie privée. Autrement dit, le juge va décider si les caméras « augmentées » sont le meilleur moyen pour parvenir au but recherché par l'Administration.

Ces deux recours devant le juge administratif participent du bon déroulement de l'expérimentation des caméras « augmentées » puisqu'ils vont permettre de déterminer concrètement les limites de leur déploiement et ainsi encadrer le pouvoir d'appréciation de l'Administration de la loi JOP. Selon l'interprétation retenue le déploiement de ces dispositifs intelligents pourrait être extrêmement étendu ce qui ne pourrait pas apparaître proportionné au regard des différents enjeux en présence. Les contentieux concernant le logiciel Briefcam sont une première illustration du type de contentieux possible lors du déploiement des caméras « augmentées ».

¹³⁴ Article L.521-1 CJA : « Quand une décision administrative, même de rejet, fait l'objet d'une requête en annulation ou en réformation, le juge des référés, saisi d'une demande en ce sens, peut ordonner la suspension de l'exécution de cette décision, ou de certains de ses effets, lorsque l'urgence le justifie et qu'il est fait état d'un moyen propre à créer, en l'état de l'instruction, un doute sérieux quant à la légalité de la décision. / Lorsque la suspension est prononcée, il est statué sur la requête en annulation ou en réformation de la décision dans les meilleurs délais. La suspension prend fin au plus tard lorsqu'il est statué sur la requête en annulation ou en réformation de la décision ».

B. L'exemple des contentieux Briefcam

Le logiciel Briefcam est développé depuis 2008 par la société israélienne du même nom. Ce logiciel va analyser les images collectées par les caméras de vidéoprotection afin de reconnaître un véhicule via sa plaque d'immatriculation ou bien d'identifier une personne grâce à ses vêtements. De plus, ce logiciel offre une fonctionnalité de reconnaissance faciale. Cette dernière fonctionnalité a fait parler d'elle depuis que l'enquête de Disclose a révélé qu'elle était utilisée par les forces de sécurité intérieure depuis 2015 sans cadre légal¹³⁵. Plusieurs recours ont été intentés contre l'usage de la reconnaissance faciale dans plusieurs communes de France : Caen¹³⁶, Nice¹³⁷, et Lille¹³⁸.

Ces trois tribunaux administratifs ont rendu des décisions différentes puisque celui de Caen a accueilli favorablement la requête, avant d'être contredit par le Conseil d'État en appel¹³⁹, alors que les deux autres tribunaux administratifs ont rejeté les requêtes. Les éléments communs à toutes ces décisions visent, d'une part, à distinguer la vidéosurveillance algorithmique et la reconnaissance faciale puisque les deux technologies ne sont pas interdépendantes. D'autre part, ces décisions permettent également de montrer que même si les communes peuvent avoir acquis un logiciel algorithmique qui comporte une fonctionnalité de reconnaissance faciale, la seule détention d'une telle fonctionnalité ne peut pas permettre d'interdire l'utilisation complète du logiciel dès lors que cette fonctionnalité ne peut pas être utilisée ou n'est pas utilisée par la commune.

Néanmoins, il convient de noter que ces décisions prennent leur fondement sur des faits ayant été commis avant l'adoption de la loi JOP qui a autorisé le recours à la vidéoprotection intelligente tout en maintenant interdit le recours à la reconnaissance faciale. Dès lors, la seule détention d'un logiciel algorithmique ne pourra plus être contestée seules pourront être contestés la proportionnalité d'y recourir par rapport aux intérêts en cause et également le recours à la reconnaissance faciale qui reste explicitement interdit en matière de police administrative.

¹³⁵ Article de l'enquête de Disclose : <https://disclose.ngo/fr/article/la-police-nationale-utilise-illegalement-un-logiciel-israelien-de-reconnaissance-faciale/> (consulté le 15 avril 2024).

¹³⁶ TA Caen, ord. référé, 22 novembre 2023, n° 2303004 et 2303012.

¹³⁷ TA Nice, ord. référé, 23 novembre 2023, n° 2305692, 2306593 et 2305712.

¹³⁸ TA Lille, ord. référé, 29 novembre 2023, n° 2310103 et 2310163.

¹³⁹ CE, ord. référé, 21 décembre 2023, n° 489990.

Cette première partie a permis d'étudier le nouveau régime juridique mis en place pour le déploiement des caméras « augmentées », qui est un enjeu fondamental en matière de sécurité et de liberté. En effet, les résultats de cette expérimentation vont déterminer les orientations d'un futur régime juridique relatif aux caméras « augmentées ». L'étude de ce régime juridique a permis de démontrer que les caméras « augmentées » ne vont pas porter atteinte à la liberté de manifestation puisqu'elles ne pourront pas être déployées sur d'autres « manifestations » que celles ayant un caractère sportif, récréatif et culturel. A l'inverse, leur déploiement va nécessairement porter atteinte au droit au respect de la vie privée des personnes se trouvant dans leur champ de vision puisqu'elles vont être analysées en temps réel et en permanence. Néanmoins, toutes les garanties ont été mises en place afin de s'assurer que leur déploiement soit le plus respectueux possible du droit au respect de la vie privée tout en visant à mieux garantir la sécurité de ces « manifestations », et ce même si l'interprétation de la loi qui est privilégiée peut étendre considérablement leur déploiement géographique. Toutefois, pour s'assurer d'un bon déploiement des caméras « augmentées » lors des JOP 24 il convient d'accélérer les expérimentations comme le préconise le rapport sénatorial d'Agnès CANAYER et Marie-Pierre de LA GONTRIE du 10 avril 2024¹⁴⁰.

Désormais, il convient d'élargir le champ de cette étude en ayant une perspective temporelle bien plus pérenne. En effet, la loi JOP a permis d'unifier le régime juridique de la vidéoprotection en France puisque désormais il est entièrement soumis au contrôle de la CNIL. De plus, il conviendra d'étudier le futur règlement européen sur l'IA. Celui-ci va créer un cadre juridique respectueux des droits et libertés fondamentaux puisqu'il établit des lignes rouges ainsi que des principes fondamentaux relatifs à l'IA de sa conception à sa mise sur le marché.

¹⁴⁰ (A.) CANAYER et (M.-P.) de LA GONTRIE, n° 527, 10 avril 2024, *op. cit.*, : « S'il semble que les services de la préfecture de police aient un retour d'expérience positif sur trois des cas d'usage testés, les rapporteuses considèrent que malgré l'expertise avérée des personnels en la matière, un tel outil nécessitait d'**importantes mesures de préfiguration et de réglage afin d'être pleinement efficace**. Au surplus, eu égard à la **faible ampleur du test ainsi réalisé**, il y a, aux yeux des rapporteuses, fort à craindre qu'y compris pour la préfecture de police de Paris, une telle solution ne puisse être utilement mise en œuvre à une échelle pertinente et permettant d'économiser le nombre de forces de sécurité intérieure engagée du fait de l'aide à la décision ainsi mis à leur disposition », p.48.

**TITRE II : LE RENFORCEMENT DU CONTRÔLE NON JURIDICTIONNEL
DES SYSTÈMES DE VIDÉOPROTECTION ET L'ÉLABORATION D'UNE
RÈGLEMENTATION RELATIVE À L'INTELLIGENCE ARTIFICIELLE**

TITRE II : LE RENFORCEMENT DU CONTRÔLE NON JURIDICTIONNEL DES SYSTÈMES DE VIDÉOPROTECTION ET L'ÉLABORATION D'UNE RÉGLEMENTATION RELATIVE À L'INTELLIGENCE ARTIFICIELLE

« Réalité quotidienne, l'intelligence artificielle a pourtant ceci de paradoxal qu'elle semble constamment échapper au temps présent, pour nous projeter dans un futur qui alimente, chez les uns, le rêve d'un monde parfait ou l'espoir d'une vie meilleure, chez d'autres, le cauchemar de l'asservissement de l'humanité par la machine ou la crainte de la dérive et de la manipulation mentale »¹⁴¹. Ces deux conceptions concernant l'IA ont rendu presque impossible toute réglementation de son usage étant donné qu'il s'agit d'une technologie en constante évolution technique. L'intelligence artificielle représente « un facteur de croissance économique et un enjeu stratégique »¹⁴² majeur pour le XXI^e siècle, il convient donc d'éviter les usages à risque de cette technologie en imposant une réglementation de ceux-ci. Tel est par exemple le cas du réseau social Tik Tok qui a été contraint par l'Union européenne de retirer une fonctionnalité permettant aux usagers de gagner de l'argent en fonction du temps de visionnage de vidéos¹⁴³. L'Union européenne a donc ici voulu combattre une certaine addiction que pouvait créer ce réseau social.

L'IA peut se définir comme : « un procédé logique et automatisé reposant généralement sur un algorithme et en mesure de réaliser des tâches bien définies »¹⁴⁴. Cette technologie est déjà utilisée par les pouvoirs publics, comme par exemple sur les plateformes numériques de conversation avec les usagers. L'adoption de la loi JOP a autorisé le recours au traitement algorithmique en temps réel des images collectées par les caméras de vidéoprotection, cela va accroître le recours à l'IA en matière d'ordre public ainsi que les investissements effectués en la

¹⁴¹ CE, étude à la demande du Premier ministre « Intelligence artificielle et action publique : construire la confiance, servir la performance », étude adoptée en assemblée générale plénière du 31 mars 2022, p. 16.

¹⁴² (B.) FAUVARQUE-COSSON et (A.-M.) HAZARD-TOURILLON (dir.), *Droit & Grands Enjeux du Monde Contemporain*, Turin, Nathan, 2021, p. 224.

¹⁴³ Article sur Tik Tok Lite et le système de rémunération en fonction du temps d'écran passé sur ce réseau social : <https://www.lesnumeriques.com/societe-numerique/tiktok-lite-mise-en-pause-du-systeme-de-remuneration-en-europe-n221091.html> (consulté le 24 avril 2024).

¹⁴⁴ Définition de l'intelligence artificielle selon la CNIL : <https://www.cnil.fr/fr/definition/intelligence-artificielle#:~:text=L'intelligence%20artificielle%20est%20un,r%C3%A9aliser%20des%20t%C3%A2ches%20bien%20d%C3%A9finies> (consulté le 1er avril 2024).

matière¹⁴⁵. En contrepartie de l'extension de l'usage de l'IA, la loi JOP a renforcé le contrôle non juridictionnel opéré par la CNIL dans la mise en oeuvre de tous les systèmes de vidéoprotection afin d'offrir une meilleure protection au regard du droit des données personnel. Dans le même temps, cette loi JOP est l'occasion de mettre en valeur l'aspect technique des traitements algorithmiques (Chapitre 1). En parallèle, afin que les Etats de l'Union européenne soient dotés d'un même corpus juridique relatif à l'IA, le Parlement européen a adopté le 13 mars 2024 la proposition de règlement sur ce sujet. Cette législation deviendrait la première régulant l'IA au niveau international et ayant pour objectif de développer une IA « digne de confiance »¹⁴⁶ (Chapitre 2).

Chapitre 1 : L'expérimentation des caméras « augmentées » mettant en valeur cette technologie et le rôle de la CNIL

La CNIL est une autorité administrative indépendante créée par la loi « Informatique et Libertés ». Elle a pour mission d'être le « régulateur des données personnelles »¹⁴⁷. Autrement dit, elle va veiller à ce que les professionnels traitent les données personnelles conformément aux règles en vigueur et elle aide aussi les particuliers pour défendre leurs droits dans le domaine du numérique. Cette Commission a également un pouvoir de sanction, renforcé par la loi pour une République numérique¹⁴⁸, comme cela a été perçu au travers du contentieux Clearview AI¹⁴⁹. Enfin, elle a pour mission d'anticiper et d'innover, c'est-à-dire qu'elle va participer aux différents débats de société concernant les données personnelles. Cette mission s'est particulièrement illustrée lors de l'adoption de la loi JOP puisque la CNIL a adopté une position sur le déploiement des caméras « augmentées » en juillet 2022 qui se fondait sur les réponses provenant de la consultation publique qu'elle avait initiée au début de la même année. Cette position a été fondamentale dans les choix

¹⁴⁵ (E.) SERUGA-CAU, « L'utilisation de « caméras augmentées » dans l'espace public ... », *op. cit.*, « À titre d'exemple, 75 % du Fonds interministériel de prévention de la délinquance (FIPD) devraient être consacrés au déploiement de la vidéoprotection en 2023 », p. 1.

¹⁴⁶ Résolution législative du Parlement européen du 13 mars 2024 sur la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle, considérant n° 7.

¹⁴⁷ Site de la CNIL, rubrique « missions » : <https://cnil.fr/fr/la-cnil/les-missions-de-la-cnil> (consulté le 18 avril 2024).

¹⁴⁸ Loi n° 2016-1321 du 7 octobre 2016 *pour une République numérique*.

¹⁴⁹ *Supra*, A. Le respect du droit à l'anonymat des personnes soumises aux caméras « augmentées », p. 39.

retenus dans la loi JOP pour l'expérimentation des caméras intelligentes. En effet, le législateur a retenu la technologie des caméras « augmentées » et non des caméras biométriques, ces dernières présentant un « degré d'intrusivité »¹⁵⁰ supérieur. La CNIL est ainsi apparue comme un « régulateur, soucieux de conjuguer le développement de notre pays par le soutien à l'innovation et le respect des droits fondamentaux des personnes concernées, et un facilitateur de l'innovation technologique au service de la société, soucieux de créer un environnement favorable à l'innovation responsable »¹⁵¹.

La loi JOP a permis de mettre en valeur l'aspect technique lié au développement des traitements algorithmiques liés aux caméras « augmentées » (section 1). De même, cette loi a unifié les régimes juridiques relatifs aux systèmes de vidéoprotection sous le contrôle de la CNIL et a ainsi offert à cette Commission un rôle majeur dans l'évaluation de l'expérimentation des caméras « augmentées » (Section 2).

Section 1 : Une appréhension technique de l'intelligence artificielle au travers des caméras « augmentées »

Avant d'être un outil au profit de la sécurité des grands événements, les caméras « augmentées » sont des outils technologiques dotés d'une intelligence artificielle reposant sur des traitements algorithmiques. Ces traitements algorithmiques vont être conçu afin de détecter les évènements prédéterminés qui se trouvent dans le décret du 28 août 2023 (Paragraphe 1). La détection de ces situations anormales repose sur de l'entraînement des algorithmes sur la base d'échantillons de données, lesquels doivent respecter différentes conditions afin de ne pas entraîner de décisions discriminatoires (Paragraphe 2).

¹⁵⁰ CNIL, Position sur les conditions de déploiement : caméras dites « intelligentes » ou « augmentées » dans les espaces publics, juillet 2022, p. 10.

¹⁵¹ CE, étude à la demande du Premier ministre « Intelligence artificielle et action publique : *op. cit.* », étude adoptée en assemblée générale plénière du 31 mars 2022, p. 202.

Paragraphe 1 : La détection de situations anormales par les caméras « augmentées »

Comme cela a été étudié dans la première partie¹⁵², les caméras « augmentées » ont pour rôle d’alerter la personne surveillant les écrans de vidéoprotection lorsqu’une situation anormale se produit, selon les événements prédéterminés que l’algorithme doit détecter. Pour cela, il faut utiliser une technologie qui corresponde aux exigences techniques imposées par la loi JOP afin de respecter les droits et libertés fondamentaux des personnes. Tel est le cas du logiciel Cityvision qui a été utilisé lors d’une expérimentation des caméras « augmentées » afin de sécuriser le match de Football PSG-OL en avril 2024¹⁵³.

Selon le site internet Wintics, ce logiciel semble remplir plusieurs conditions requises pour être déployé lors des expérimentations des caméras « augmentées ». En effet, ce logiciel peut être déployé dans l’espace public ainsi que dans les lieux de transport public afin de détecter en temps réel des « situations dangereuses »¹⁵⁴ comme par exemple l’intrusion dans une zone interdite ou bien le non-respect du sens de circulation par une personne ou un véhicule. Dans ce second cas, il convient selon la CNIL qu’un sens de circulation soit préalablement imposé aux usagers notamment par la présence d’un panneau « sens interdit ». Du point de vue des caméras « augmentées », le traitement algorithmique devra contenir une fonctionnalité permettant de définir un sens de circulation conforme aux règles prévues dans ce domaine. Tel est le cas pour le logiciel Briefcam qui détient un filtre *Line crossing*, lequel permet de tracer une ligne virtuelle dans le logiciel en indiquant le sens de circulation incorrect qu’il convient de détecter, selon le positionnement de la caméra¹⁵⁵.

Enfin, concernant le signalement d’attention effectué par les caméras « augmentées », celui-ci peut s’effectuer comme l’illustre l’annexe VI de ce mémoire provenant de la CNIL. En l’espèce, une personne circule à vélo dans une zone interdite aux vélos ce qui produit un signalement

¹⁵² *Supra*. B. La fonction d’alerte des caméras « augmentées ».

¹⁵³ Arrêté, n° 2024-00493, *op. cit.*

¹⁵⁴ Site Wintics page collectivités : <https://wintics.com/collectivites/> (consulté le 23 avril 2024).

¹⁵⁵ Vidéo du filtre *Line crossing* sur le logiciel Briefcam : <https://www.briefcam.com/resources/videos/detecting-traffic-violations-with-briefcam/> (consulté le 24 avril 2024).

d'attention au profit de la personne chargée de surveiller les écrans retransmettant les images de vidéoprotection afin qu'il puisse déterminer l'action à mener.

Afin d'avoir un traitement algorithmique efficace et sans prise de décision discriminatoire il convient, lorsque l'algorithme le requiert, de lui fournir des données qui soient pertinentes et adéquates.

Paragraphe 2 : Le développement du traitement algorithmique pour l'expérimentation des caméras « augmentées » au travers de l'utilisation des données

Le développement des traitements algorithmiques et les différentes expérimentations menées visent à les rendre opérationnels pour les JOP 24. Les éléments essentiels pour perfectionner ces algorithmes sont les données utilisées. Le développement de cet algorithme comprends trois phases successives (conception, développement et exploitation) comme le relève le Conseil d'État dans son avis du 15 décembre 2022¹⁵⁶. Pour ces différentes phases de développement d'un algorithme, l'élément essentiel repose sur les données qui seront intégrées dans ce logiciel.

En effet, afin que l'algorithme soit efficace il convient d'établir un échantillon de données pertinent. Cet échantillon va être composé d'images collectées par les systèmes de vidéoprotection pendant l'entraînement de l'algorithme, ainsi que par des images collectées lors des multiples expérimentations des caméras « augmentées » qui se déroulent¹⁵⁷ et se multiplient¹⁵⁸. Dans ces deux hypothèses, l'échantillon de données doit répondre à diverses conditions prévues au paragraphe VI de l'article 10 de la loi JOP. Les données utilisées dans ce cadre doivent satisfaire aux exigences de « pertinence, d'adéquation et de représentativité ». En tout état de cause, l'objectif est de constituer un échantillon d'images collectées par les caméras « augmentées » n'entraînant pas d'alertes

¹⁵⁶ CE, avis n° 406383, 15 décembre 2022, §. 25.

¹⁵⁷ Comme le prévoit le § IX de l'article 10 de la loi JOP.

¹⁵⁸ (M.) DESMURAUX, « La SNCF et la RATP autorisées à expérimenter la vidéosurveillance "intelligente" à Paris entre le 19 et le 22 avril 2024 », AEF Info, n° 710927, 17 avril 2024.

discriminatoires¹⁵⁹, conformément aux 25 critères que reconnaît le droit français¹⁶⁰. Concernant les données utilisées à la suite de leur collecte lors d'une expérimentation, le paragraphe IX de l'article 10 prévoit qu'elles ne peuvent être conservées que pour une durée de douze mois et qu'elles doivent être détruites à la fin de l'expérimentation dans le but de préserver le droit au respect de la vie privée des personnes dont les images sont utilisées comme donnée d'entraînement.

Un échantillon de données d'entraînement est utilisé uniquement lorsque l'algorithme repose sur l'apprentissage automatique - ou *machine learning* -, c'est-à-dire que l'on va donner aux algorithmes des données afin qu'ils apprennent eux-mêmes quelles sont les informations pertinentes à tirer à partir des données. Pour l'utilisation des données collectées lors des différentes expérimentations, la loi JOP prévoit qu'elles doivent faire l'objet d'une pseudonymisation ainsi que d'un floutage dans la mesure du possible. Pour que l'algorithme soit le plus efficace possible lors des JOP 24, l'échantillon des données est très important puisqu'il ne faut pas qu'il crée de biais dans l'algorithme tel que le biais de *garbage in, garbage out*, c'est-à-dire qu'il ne faut pas que la donnée d'entraînement soit mauvaise sinon le résultat en sortie sera également mauvais. Il ne faut pas non plus qu'une donnée oublie une variable telle que l'ethnie sinon cela pourrait aboutir à des alertes discriminatoires.

Enfin, l'algorithme doit pouvoir être interrompu à tout moment par une personne humaine. Cette obligation suit la logique générale de l'utilisation de l'intelligence artificielle en France qui doit rester sous le contrôle humain à tout moment et ne doit pas fonder de décisions individuelles par lui-même, mais n'être qu'une simple aide à la décision humaine¹⁶¹.

¹⁵⁹ « En réalité, il n'y a ni magie technologique ni neutralité mathématique : les algorithmes sont conçus par des humains et à partir de données reflétant des pratiques humaines. Ce faisant, des biais peuvent être ainsi intégrés à toutes les étapes de l'élaboration et du déploiement des systèmes [...] », rapport du Défenseur des droits, « Algorithmes : prévenir l'automatisation des discriminations », 2020, p. 4.

¹⁶⁰ Annexe VII : Infographie sur les 25 critères de discrimination reconnus par la loi française.

¹⁶¹ « [...] Si l'on peut, par de nouvelles technologies, apporter une aide à la décision des ressources humaines, il ne faut pas s'en priver, moyennant, bien évidemment, toutes les garanties nécessaires », rapport n° 939 de l'Assemblée nationale, (G.) VUILLETET, p.442.

Section 2 : Le rôle central de la CNIL dans le contrôle des systèmes de vidéoprotection

La loi JOP a mis fin à une dualité de régime juridique, en matière de vidéoprotection, jugée « obsolète » par la CNIL¹⁶². Désormais tous les systèmes de vidéoprotection sont soumis au droit des données à caractère personnel (Paragraphe 1). Par ailleurs, la loi JOP a octroyé à la CNIL un rôle majeur dans l'évaluation de l'expérimentation des caméras « augmentées » dans le but de mieux définir le futur cadre juridique en la matière (Paragraphe 2).

Paragraphe 1 : L'unification des régimes juridiques de la vidéoprotection au profit de leur soumission au droit des données à caractère personnel

Cette dualité de régime juridique, en matière de vidéoprotection, existait depuis la LOPS de 1995. En effet, cette loi distinguait les systèmes de vidéoprotection selon qu'ils avaient pour finalité d'utiliser les images collectées dans un traitement automatisé afin d'identifier les personnes physiques et ceux qui n'avaient pas cette finalité. Les premiers étaient soumis à la loi du 6 janvier 1978¹⁶³, c'est-à-dire au droit des données à caractère personnel, alors que les seconds n'y étaient pas soumis. Les seconds types de systèmes de vidéoprotection étaient uniquement soumis aux articles L.251-1 anciens et suivants du CSI qui ne leur conféraient pas le statut de données à caractère personnel.

L'article 10 de la loi JOP a fusionné les deux régimes au profit d'une meilleure protection des images collectées par des systèmes de vidéoprotection en soumettant l'ensemble de ces systèmes à la loi « Informatique et Libertés », ainsi qu'au RGPD¹⁶⁴. Cela est donc davantage

¹⁶² CNIL, délibération n°2022-043 du 14 avril 2022 portant avis sur un projet de décret relatif à l'extension des destinataires d'images de vidéoprotection : « La Commission rappelle plus largement la nécessité de prévoir rapidement un cadre juridique cohérent, complet et suffisamment protecteur des droits des personnes en matière de vidéoprotection. En effet, de nombreuses dispositions du CSI, qui constituent le cadre juridique général en la matière, sont obsolètes depuis l'évolution de la réglementation en matière de protection des données à caractère personnel intervenue en 2018 ».

¹⁶³ Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*.

¹⁶⁴ (G.) VUILLETET, rapport n°939 de l'Assemblée Nationale, fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, sur le projet de loi, adopté par le Sénat après engagement de la procédure accélérée, relatif aux jeux Olympiques et Paralympiques de 2024, et portant diverses autres dispositions, p.60.

protecteur du droit au respect de la vie privée puisque la CNIL est compétente pour contrôler l'ensemble des systèmes de vidéoprotection.

La fin de la dualité des régimes juridiques relatifs à la vidéoprotection a été effectuée par la loi JOP. Néanmoins, celle-ci était devenue obsolète depuis l'arrêt de la Cour de Justice de l'Union européenne du 11 décembre 2014 qui a considéré que : « l'exploitation d'un système de caméra, donnant lieu à un enregistrement vidéo des personnes stocké dans un dispositif d'enregistrement continu tel qu'un disque dur, installé par une personne physique sur sa maison familiale afin de protéger les biens, la santé et la vie des propriétaires de la maison, ce système surveillant également l'espace public, ne constitue pas un traitement des données effectué pour l'exercice d'activités exclusivement personnelles ou domestiques, au sens de [l'article 3, paragraphe 2, second tiret, de la directive 95/46] »¹⁶⁵. En l'espèce, un particulier avait installé une caméra de surveillance dans sa maison, mais celle-ci filmait également la voie publique et la propriété de ses voisins. La question préjudicielle posée à la Cour de Justice de l'Union européenne consistait à déterminer si un tel usage d'un système de vidéosurveillance pouvait intégrer les exceptions inscrites dans la directive 95/46¹⁶⁶ et donc ne pas constituer un traitement de données à caractère personnel, ou bien si cet usage constituait un traitement de données à caractère personnel soumis à cette directive. Pour considérer que cet usage de caméra de surveillance constituait un traitement de données à caractère personnel, la Cour de Justice de l'Union européenne interprète de manière stricte les exceptions prévues dans la directive ce qui est donc protecteur du droit au respect de la vie privée des personnes filmées et dont l'image est collectée. Cette décision a connu une nouvelle actualité puisque le RGPD a abrogé la directive 95/46. Les systèmes de vidéoprotection sont désormais soumis au droit des données à caractère personnel, représenté par le RGPD qui est inclus dans la loi « Informatique et Libertés » avec pour complément la directive « police-justice » du 27 avril 2016¹⁶⁷.

¹⁶⁵ CJUE, 11 décembre 2014, C-212/13.

¹⁶⁶ Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

¹⁶⁷ Directive (UE) 2016/680 du 27 avril 2016 dite « police-justice ».

Paragraphe 2 : Le rôle de la CNIL dans l'évaluation de l'expérimentation des caméras « augmentées »

L'évaluation est la conclusion indispensable d'une expérimentation¹⁶⁸, celle-ci va participer au devenir du régime juridique qui a été introduit de manière temporaire. Sans cette évaluation l'expérimentation n'a pas de sens. De même l'évaluation doit être menée avec des critères cohérents et pertinents sinon il y a un risque de mal évaluer l'expérimentation, ce qui est pire que l'absence d'évaluation selon (V.) LASSERRE¹⁶⁹.

Le paragraphe XI de l'article 10 de la loi JOP offre à la CNIL un rôle central dans l'ensemble de l'expérimentation des caméras « augmentées » et notamment lors de l'évaluation générale de celle-ci. Tout d'abord, la CNIL est informée de toutes les mises en oeuvre des caméras « augmentées » au travers des analyses d'impact sur la protection des données (AIPD) que doivent établir les responsables de traitement lors de la mise en oeuvre des caméras « augmentées »¹⁷⁰.

Par ailleurs, la loi JOP octroie un rôle à cette Commission dans la fixation du contenu du rapport émis par le Gouvernement à destination du Parlement et de cette Commission, au plus tard le 31 décembre 2024. En effet, le contenu du rapport fut fixé dans un décret dont la publication est intervenue le 11 octobre 2023¹⁷¹. L'article 4 de ce décret précise l'ensemble du contenu du rapport. Ce dernier : « 1° Recense le nombre de demandes d'autorisations d'emploi de traitements algorithmiques par type de manifestation, le nombre d'autorisations refusées ou modifiées ainsi que leur répartition géographique et le nombre d'utilisations effectives de ces traitements, la durée moyenne de l'autorisation ; 2° Recense, par évènement dont la détection a été autorisée, le nombre

¹⁶⁸ « La norme juridique n'est donc pas édictée ni pensée comme définitive, mais comme un essai soumis à examen » (DRAGO, Le droit de l'expérimentation, in L'avenir du droit, Mélanges Terré, 1999, Dalloz, PUF, Juris-Classeur, p. 229 s., in Répertoire de droit civil, Loi et règlement – Naissance des lois et des règlements – (V.) LASSERRE – Juillet 2015 (actualisation : Janvier 2016)

¹⁶⁹ (V.) LASSERRE, Répertoire de droit civil, Loi et règlement, Naissance des lois et des règlements, Juillet 2015 (actualisation : Janvier 2016), § 227.

¹⁷⁰ Arrêté, n°2024-00493 *op. cit.*, : « Considérant, en outre, que l'emploi de ce traitement a fait l'objet d'une transmission le 12 avril 2024 par la direction de la sûreté de la SNCF, responsable de celui-ci au sens de l'article 10 de la loi du 19 mai 2023 susvisée, à la Commission nationale de l'informatique et des libertés d'un engagement de conformité au décret du 28 août 2023 susvisé, ainsi que d'une analyse d'impact sur la protection des données à caractère personnel présentant les caractéristiques particulières de ce traitement qui ne figurent pas dans l'analyse d'impact-cadre transmise par le ministère de l'intérieur et des outre-mer à cette même Commission ; ».

¹⁷¹ Décret n° 2023-939 du 11 octobre 2023 relatif aux modalités de pilotage et d'évaluation de l'expérimentation de traitements algorithmiques d'images légalement collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs.

de signalements émis par les traitements, leur pertinence ou non après vérification humaine, ainsi que les suites leur ayant été apportées ; 3° Évalue l'impact des traitements sur la sécurité des manifestations concernées ainsi que les bénéfices constatés ou les difficultés rencontrées en vue de préconiser, le cas échéant, toutes recommandations permettant l'amélioration du dispositif ; 4° Apprécie les conditions dans lesquelles il a été procédé à l'information du public et à la mise en œuvre des droits des personnes concernées ; 5° Évalue le degré de satisfaction et de confiance du public et des personnels des services ayant employé les traitements algorithmiques, en analysant les résultats de la consultation mentionnée au I ». Autrement dit, le rapport va prendre en compte l'ensemble des expérimentations menées et refusées avec les justifications permettant ou interdisant le déploiement des caméras « augmentées ». Il va également prendre en compte et constater la mise en œuvre du droit d'information au public, qui est un élément essentiel pour assurer le lien de confiance entre le public et l'autorité publique, au travers notamment d'affiches et de QRcodes comme cela fut le cas pour l'expérimentation des caméras « augmentées » lors du match de football PSG-OL. Par ailleurs, le rapport va évaluer l'impact des caméras « augmentées » sur la sécurisation des grands événements et une comparaison sera donc possible entre les événements ayant pu recourir aux caméras « augmentées » et ceux n'ayant pas eu cet outil afin de déterminer si elles ont pu jouer un rôle majeur dans leur sécurisation. Cela va donc permettre de déterminer quelles sont les perspectives en la matière ainsi que les modifications qui devront être apportées dans leur mise en œuvre, afin d'améliorer cette technologie de protection avant une généralisation dans les prochaines années.

Avant que le régime juridique des caméras « augmentées » ne soit pérennisé en France, l'Union européenne va se doter de la première législation sur l'intelligence artificielle au monde et cela va donc conditionné les éventuelles modifications à apporter aux caméras « augmentées ». Il convient donc désormais de s'intéresser à cette nouvelle réglementation en étudiant également les positions de différents pays en la matière.

Chapitre 2 : Vers une réglementation de l'intelligence artificielle au niveau européen

« Les possibilités offertes par l'intelligence artificielle connaissent peu de limites »¹⁷², c'est en partie pour cette raison qu'il existe différentes conceptions relatives à son usage selon l'État en matière de vidéoprotection. Le constat initial à ce sujet repose sur le fait que depuis les années 1990 le nombre de caméras de vidéoprotection n'a cessé de croître en Europe et dans le monde. La France n'échappe pas à ce phénomène. Le nombre de caméras de vidéoprotection sur le territoire national français ne peut être précisément connu. De fait, les représentants de l'Etat dans le département créent uniquement des zones vidéoprotégées sans indiquer le nombre précis de caméras qui sécurisent cette zone. Ce problème statistique a été mis en exergue dans un rapport parlementaire¹⁷³, lequel préconise de réaliser une « cartographie nationale de l'emplacement de toutes les caméras de vidéoprotection installées sur l'ensemble du territoire »¹⁷⁴. Néanmoins, selon différentes estimations il y aurait environ 2 millions de caméras de vidéoprotection en France. Ce nombre ne reflète pas les disparités selon les communes par rapport au nombre de caméras installées. En effet, la ville de Nice ainsi que la Préfecture de police de Paris avec son plan de vidéoprotection comptent respectivement 4000 caméras de vidéoprotection, avec des disparités relatives à leur emplacement dans la commune parisienne¹⁷⁵. Avec la loi JOP, la France s'est dotée de son premier cadre juridique relatif à l'usage de l'intelligence artificielle au sujet de la vidéoprotection.

Le législateur français est une « source d'inspiration »¹⁷⁶ au niveau européen en matière de protection des données avec la loi Informatique et Libertés. Il peut également le devenir en matière

¹⁷² Répertoire IP/IT et Communication Les biais de l'intelligence artificielle : quels enjeux juridiques ? – (G.) HAAS ; (S.) ASTIER – Juillet 2019, § 19.

¹⁷³ « Cependant, l'absence de registres précis et exhaustifs présentant l'emplacement de toutes les caméras de vidéoprotection déployées sur le territoire national demeure problématique », p. 114, Assemblée nationale, Rapport d'information n° 1089 sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité, (P.) GOSSSELIN et (P.) LATOMBE.

¹⁷⁴ *Ibid*, recommandation n°34.

¹⁷⁵ Annexe VIII : Cour des comptes, carte de la répartition des caméras de vidéoprotection par arrondissement de Paris, référé : le plan de vidéoprotection de la préfecture de police de Paris, 2 décembre 2021.

¹⁷⁶ Répertoire IP/IT et Communication Les biais de l'intelligence artificielle : quels enjeux juridiques ? – (G.) HAAS ; (S.) ASTIER – Juillet 2019, § 6.

d'IA puisqu'il permet de déployer de grands principes en cette matière au regard des droits fondamentaux, c'est dans cette perspective que s'est déroulée l'adoption de la proposition de règlement européen sur l'IA le 13 mars 2024. Ce règlement a pour objectif de créer un cadre juridique digne de confiance, c'est-à-dire éthique et respectant les droits et libertés fondamentaux. Le règlement est une norme juridique d'origine européenne définie à l'article 288 alinéa 2 du Traité sur le fonctionnement de l'Union européenne, lequel dispose : « Le règlement a une portée générale. Il est obligatoire dans tous ses éléments et il est directement applicable dans tout État membre ». Autrement dit, un règlement est impératif pour les États membres de l'Union européenne, ils n'ont aucune marge de manoeuvre dans l'application de celui-ci.

Ce règlement européen englobe divers secteurs économiques relatifs à l'IA tel que le développement ainsi que la mise sur le marché de cette technologie. Malgré ces différents aspects, le règlement établit différentes interdictions concernant l'usage de l'IA (Section 1). Ces interdictions visent à créer un cadre juridique digne de confiance au niveau européen, notamment en respectant les valeurs fondamentales de l'Union européenne (Section 2).

Section 1 : L'établissement de lignes rouges dans l'utilisation de l'intelligence artificielle

Le règlement européen sur l'IA prévoit dès son commencement les « lignes rouges »¹⁷⁷ à ne pas franchir dans le développement et la mise sur le marché de cette technologie. Ces lignes rouges ont pour finalité de créer de la confiance dans le recours à l'IA dans les différents secteurs économiques ainsi qu'en matière de sécurité publique. En effet, ce règlement s'applique à la fois aux acteurs privés et acteurs publics. Pour restreindre les cas d'usages de l'IA en matière de sécurité, le règlement prévoit l'interdiction de classer socialement les personnes (Paragraphe 1). De même, ce texte prévoit que pour un usage éthique de l'IA, il faut qu'elle ait des finalités précises à respecter (Paragraphe 2).

¹⁷⁷ Sénat, rapport d'information n° 627 fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles, par les sénateurs DAUBRESSE (M.-P.) BELENET (A.) et DURAIN (J.), 10 mai 2022, p. 8.

Paragraphe 1 : L'interdiction de classer socialement les personnes

L'interdiction de classer socialement les personnes peut se scinder en deux objets distincts. Tout d'abord, cette interdiction entraîne l'impossibilité de recourir à une notation sociale des personnes au niveau européen et cela dans le but de lutter directement contre le modèle chinois en la matière.

Selon le représentant permanent de la France auprès de l'Union européenne, le règlement européen sur l'IA « est conçu comme une réponse politique de l'Europe au système de contrôle social chinois »¹⁷⁸. La Chine utilise depuis 2014¹⁷⁹ l'intelligence artificielle, et plus particulièrement la reconnaissance faciale, afin de noter son peuple dans le but de le surveiller dans son quotidien. Ce système est particulièrement bien décrit dans le documentaire « Ma femme a du crédit », dans lequel le journaliste suit sa femme dans son quotidien et montre que la reconnaissance faciale permet à cette dernière d'effectuer toutes ses actions habituelles, lesquelles actions lui rapportent des points selon leur bien fondé. Finalement, ces points permettent de classer cette citoyenne chinoise comme un bon ou un mauvais citoyen. Ce système vise à augmenter le niveau de vertu des citoyens et repose essentiellement sur la reconnaissance faciale. Par exemple dans le documentaire précité lorsqu'un citoyen ne respecte pas le code de la route en tant que piéton, une photographie de sa personne est affichée sur de grands écrans dans la rue afin d'instaurer une réprobation sociale ainsi que de lui faire perdre des points pour cette mauvaise action. Le fait pour un citoyen chinois de perdre des points va avoir des conséquences concrètes dans sa vie quotidienne puisqu'il subira, par exemple, des restrictions dans l'accès au transport¹⁸⁰. L'Occident veut combattre cet usage de la reconnaissance faciale et plus largement de l'IA, comme le montre le rapport d'information du Sénat relatif à la reconnaissance faciale. Ce dernier recommande l'interdiction pure et simple d'une telle utilisation de l'intelligence artificielle¹⁸¹. De même, cette recommandation est reprise dans le règlement européen sur l'IA puisque cet usage se trouve à l'article 5 du règlement, lequel se situe dans le chapitre relatif aux « pratiques interdites en matière d'intelligence artificielle ». Dès lors, au

¹⁷⁸ *Ibid*, p. 46.

¹⁷⁹ *Ibid*, p. 30.

¹⁸⁰ Communiqué de la Commission nationale du développement de la réforme, <https://www.chinatax.gov.cn/n810341/n810755/c3359637/content.html> (consulté le 28 avril 2024).

¹⁸¹ Sénat, rapport n° 627, *op. cit.*, p. 11.

niveau européen tous les systèmes d'IA qui seront produits et mis sur le marché ne pourront détenir une quelconque fonctionnalité ayant pour but de noter socialement les individus afin de les classer pour leur attribuer tel droit plutôt que tel autre en fonction de leur comportement. En effet, le comportement d'une personne est une donnée sensible selon le RGPD et son traitement est très encadré voire interdit comme pour l'expérimentation des caméras « augmentées »¹⁸². Une telle utilisation de l'IA en Chine participe d'une violation particulièrement importante des droits fondamentaux des personnes comme le droit au respect de la vie privée et notamment le droit à l'anonymat dans l'espace public. C'est pour cette raison que l'Union européenne a voulu préciser dès le début de son règlement sur l'intelligence artificielle que cette technologie ne pourra pas être utilisée afin de classer socialement les citoyens en leur accordant tel ou tel droit selon leur comportement qu'il soit bon ou mauvais.

Par ailleurs, l'interdiction de classer socialement les personnes revient à ne pas recourir, grâce à l'intelligence artificielle, à des données qualifiées de discriminatoires. L'article 21 de la Charte des droits fondamentaux de l'Union européenne pose le principe de non-discrimination¹⁸³. Ce principe se retrouve dans le règlement européen sur l'IA, article 5 paragraphe G, puisqu'il interdit à l'intelligence artificielle de recourir aux données biométriques des personnes pour obtenir des données discriminantes et catégoriser les individus sur cette base. Cette interdiction s'inscrit dans le cadre plus général de la construction d'un droit portant sur l'IA qui soit digne de confiance puisque cela va empêcher, notamment, de produire des statistiques ethniques conformément à l'article 8 de la loi Informatique et Liberté qui fait application du RGPD¹⁸⁴. De même, cette interdiction participe à écarter « le risque d'une société de surveillance »¹⁸⁵ orwellienne ou chinoise.

¹⁸² *Supra*, A. L'absence textuelle de recours aux données biométriques et à la reconnaissance faciale.

¹⁸³ Article 21 de la Charte des droits fondamentaux de l'Union européenne : « 1. Est interdite, toute discrimination fondée notamment sur le sexe, la race, la couleur, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap, l'âge ou l'orientation sexuelle. / 2. Dans le domaine d'application du traité instituant la Communauté européenne et du traité sur l'Union européenne, et sans préjudice des dispositions particulières desdits traités, toute discrimination fondée sur la nationalité est interdite ».

¹⁸⁴ Article 8 Loi Informatique et Libertés : « I. - Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci ».

¹⁸⁵ Sénat, rapport n°627, *op. cit.*, p. 17.

Paragraphe 2 : Les différentes finalités possibles pour le recours à l'intelligence artificielle

Le déploiement des caméras de vidéoprotection en Europe et dans le monde offre de nouvelles opportunités en matière d'intelligence artificielle. En effet, la multiplication des caméras de vidéoprotection dans des villes comme Londres¹⁸⁶, laquelle est entourée par ce qui est appelé un anneau d'acier composé essentiellement de caméras de vidéoprotection, permet d'envisager l'usage de l'IA afin de rationaliser le travail des personnes chargées de surveiller les écrans transmettant les images de vidéoprotection.

Il convient tout d'abord de distinguer les IA faibles des IA fortes. Une IA forte est destinée à réaliser différentes tâches comme un être humain, elle n'est pas spécialisée. À l'inverse, une IA faible est conçue sur la base d'un algorithme destiné à réaliser une tâche prédéfinie. Il s'agit d'une IA experte dans son domaine mais qui ne peut pas réaliser d'autres tâches. C'est ce second type d'IA qui est utilisé dans l'expérimentation des caméras « augmentées » ainsi que dans le règlement européen sur l'IA puisque ces textes octroient à l'intelligence artificielle des finalités précises. Ces IA ne peuvent donc pas réaliser d'autres tâches non prévues lors de leur développement. C'est en raison de cela que les caméras « augmentées » ne pourront détecter que les événements prédéterminés dans le décret d'application de la loi JOP.

L'IA faible peut avoir différentes finalités. En matière de vidéoprotection intelligente, lors de leur expérimentation les caméras « augmentées » auront une finalité de police administrative. En effet, elles doivent permettre de mieux garantir la sécurité des manifestations sportives, récréatives et culturelles en prévenant les troubles les plus graves à l'ordre public.

Un autre finalité de l'IA consiste, grâce à la reconnaissance faciale, à authentifier et à identifier une personne au sein d'une foule à des fins de police judiciaire. Cette finalité n'est pas octroyée aux caméras « augmentées » lors de leur expérimentation puisqu'il s'agit uniquement d'un dispositif de police administrative qui peut n'être autorisé que par le représentant de l'État dans le département et non un magistrat de l'ordre judiciaire.

¹⁸⁶ Selon Courrier International, en 2019 la ville de Londres est classée sixième ville du monde avec le plus de caméras de vidéoprotection avec un total de 627 707 caméras, soit 68 caméras pour 1000 habitants.

Le règlement européen sur l'IA prévoit que par principe le recours aux données biométriques en temps réel est interdit mais prévoit trois hypothèses où celui-ci est possible et cela pourrait être utilisé en matière de vidéoprotection. Ces exceptions prennent place dans la finalité judiciaire. Tout d'abord, l'usage des données biométriques en temps réel sera possible pour rechercher les victimes d'infractions spécifiques graves (traite d'êtres humains, enlèvement) ou bien pour les personnes portées disparues. De même, cela sera utilisable afin de rechercher les auteurs d'infractions punies d'au moins quatre ans d'emprisonnement. Enfin, la dernière finalité porte sur la prévention d'actes de terrorisme, dès lors cette hypothèse serait sans doute plus appropriée dans une finalité de police administrative comme cela est déjà prévue pour les caméras « augmentées ».

En tout état de cause, ces différentes finalités de l'IA supposent le recours à la reconnaissance faciale, fonctionnalité qui est toujours interdite en France en matière de vidéoprotection. Il serait donc intéressant de voir à la fin de l'expérimentation des caméras « augmentées » si le rapport d'évaluation préconise l'usage de la reconnaissance faciale comme cela est prévue dans le règlement européen ou bien si le rapport se rapproche de la position traditionnelle de la CNIL et du législateur français qui ont une position défavorable au déploiement de la reconnaissance faciale en matière d'ordre public. En plus, de ces différentes restrictions tenant à l'usage de l'IA, le règlement européen prévoit d'établir un cadre juridique digne de confiance.

Section 2 : L'établissement d'un cadre juridique « digne de confiance »¹⁸⁷

L'établissement d'un cadre juridique éthique au niveau européen repose à la fois sur les limitations déjà étudiée mais également sur l'élaboration de principes généraux relatifs à l'IA. Ces principes généraux sont au nombre de sept et il est possible de les classer selon qu'ils s'intéressent à la personne humaine (Paragraphe 1), ou bien qu'ils portent davantage sur l'IA en tant que tel (Paragraphe 2).

Paragraphe 1 : Les principes généraux du règlement européen sur l'intelligence artificielle relatifs à la personne humaine

Le premier principe relatif à la personne humaine consiste dans le respect de la primauté de la personne humaine dans l'utilisation de l'intelligence artificielle. Ce principe est explicitement inscrit au considérant 27 du règlement, lequel précise que les systèmes d'intelligence artificielle sont développés et utilisés afin de servir d'aide aux personnes. Autrement dit, les systèmes d'intelligence artificielle peuvent être plus ou moins autonomes mais doivent rester sous le contrôle de l'humain puisque la conception de l'IA en Europe consiste à considérer cette technologie comme étant au service de la personne humaine.

Ce principe est inscrit dans le rapport d'information n° 627 du Sénat qui insiste sur le fait que les systèmes d'intelligence artificielle doivent rester une simple « aide à la décision »¹⁸⁸. L'intelligence artificielle typique est celle qui sera utilisée dans les caméras « augmentées » puisque la loi JOP prévoit explicitement que cette technologie reste sous le contrôle d'une personne humaine. En outre, l'IA n'a pas vocation à se substituer à la décision humaine, ni même à l'influencer, elle doit simplement faciliter la prise de décision rapide d'un être humain dans une situation donnée.

Le deuxième principe relatif à la personne humaine concerne la protection des données à caractère personnel. Ce principe irrigue tout le règlement européen ainsi que les technologies d'IA de la conception au déploiement effectif. Ce règlement rappelle que les données à caractère

¹⁸⁷ Considérant 27 règlement européen sur l'IA.

¹⁸⁸ Sénat, rapport, n° 627, *op. cit.*, p.11.

personnel sont protégées par le RGPD, en France également par la loi Informatique et Libertés, et que les personnes peuvent invoquer tous les droits présents dans le RGPD en matière d'IA. L'expérimentation des caméras « augmentées » est encore un droit pionnier puisque les principes relatifs aux données d'entraînement en matière des caméras « augmentées » se retrouvent dans le règlement européen sur l'IA.

Paragraphe 2 : Les principes généraux du règlement européen ayant pour objet central l'intelligence artificielle

Les principes généraux du règlement européen portent tout d'abord sur la fiabilisation des algorithmes.

En effet, la fiabilité d'une intelligence artificielle est extrêmement importante pour que le public adhère à cette technologie surtout lorsqu'elle est utilisée afin des fins policières. Le règlement européen sur l'IA classe les IA selon le niveau de risque qu'elles font supporter aux droits et libertés fondamentaux. Tout d'abord, il y a les IA qui font peser des risques inacceptables aux droits et libertés fondamentaux. Tel est par exemple le cas des IA ayant pour finalité de manipuler les comportements. Ces IA sont totalement proscrites au niveau européen. Ensuite, il y a les IA à haut risque. Ce sont des systèmes d'intelligence artificielle qui engendrent des risques importants sur les droits et libertés fondamentaux, ils doivent donc être soumis à des exigences particulières concernant leur conformité, la protection des données utilisées ainsi que sur le contrôle humain. Ces systèmes d'intelligence artificielle sont définis à l'article 6 §2 du règlement. Enfin, le règlement consacre sa dernière catégories aux IA à faible risque pour les droits et libertés fondamentaux.

En matière de vidéoprotection intelligente, la fiabilité de la technologie repose sur les données d'apprentissage de l'algorithme afin d'éviter les différents biais préalablement évoqués.

Par ailleurs, les systèmes d'intelligence artificielle doivent être dotés d'une certaine transparence afin de garantir cette confiance nécessaire de la population envers cette technologie. La transparence des systèmes d'intelligence artificielle repose sur le fait qu'ils soient développés et utilisés afin de permettre une traçabilité de leurs interactions avec les personnes humaines.

Cette exigence de traçabilité est prévue dans la loi JOP pour l'expérimentation des caméras « augmentées » puisqu'il est prévu que le traitement algorithme enregistre automatiquement les

« signalements des événements prédéterminés détectés permettant d'assurer la traçabilité de son fonctionnement »¹⁸⁹.

CONCLUSION

Cette étude aura permis de mieux comprendre les enjeux juridiques relatifs à l'intelligence artificielle et plus particulièrement en matière de vidéoprotection. Les autorités publiques ont un devoir de maintenir l'ordre public et cette matière fait l'objet d'innovations importantes grâce à l'intelligence artificielle ainsi que par des volontés politiques de certaines communes françaises. En effet, l'édile de Nice Christian ESTROSI et Éric CIOTTI avaient proposés, en 2016¹⁹⁰, d'inclure de la reconnaissance faciale dans les caméras de vidéoprotection dans le but de procéder à une interconnexion entre les fichiers de police existants en temps réel¹⁹¹. Cette proposition a échoué puisque le Conseil constitutionnel avait préalablement décidé qu'un tel dispositif traitant des données sensibles à grande échelle porte atteinte au droit au respect de la vie privée et était donc inconstitutionnel¹⁹².

Dans ce domaine, l'innovation technologique semble à première vue faire le droit, toutefois le droit apparaît comme un régulateur des usages possibles de l'intelligence artificielle. La loi JOP participe de ce mouvement puisqu'elle autorise, sous certaines conditions strictes, le recours à l'intelligence artificielle pour mieux garantir la sécurité des manifestations sportives, récréatives et culturelles contre les atteintes les plus graves à l'ordre public. L'étude du régime juridique mis en place pour les caméras « augmentées » a permis de montrer les potentialités relatives au déploiement de ces dispositifs et les atteintes portées aux droits et libertés fondamentaux notamment le droit au respect de la vie privée. En effet, il convient de rappeler qu'en l'état actuel du régime juridique des caméras « augmentées », ces dispositifs ne portent pas atteinte à la liberté de manifestation puisque la définition juridique de ce concept ne s'applique pas aux manifestations sportives, récréatives et culturelles. C'est une limite juridique qu'il conviendra de confirmer dans

¹⁸⁹ Article 10, § VI 2° loi JOP.

¹⁹⁰ Article 20 Minutes : <https://www.20minutes.fr/nice/1854995-20160530-nice-estrosi-ciotti-ecrivent-valls-autoriser-reconnaissance-faciale> (consulté le 24 avril 2024).

¹⁹¹ (B.) CAZENEUVE et (G.) FARDE, *op. cit.*, p. 127.

¹⁹² Cons. const., n° 2012-652 DC, 22 mars 2012, *Loi relative à la protection de l'identité*.

l'évaluation de l'expérimentation des caméras « augmentées », cette limite semble extrêmement importante en démocratie puisqu'elle permet l'expression des opinions dissidentes et de s'opposer aux gouvernements. Cette limite juridique participe de la confiance que détient la population vis-à-vis de ces dispositifs.

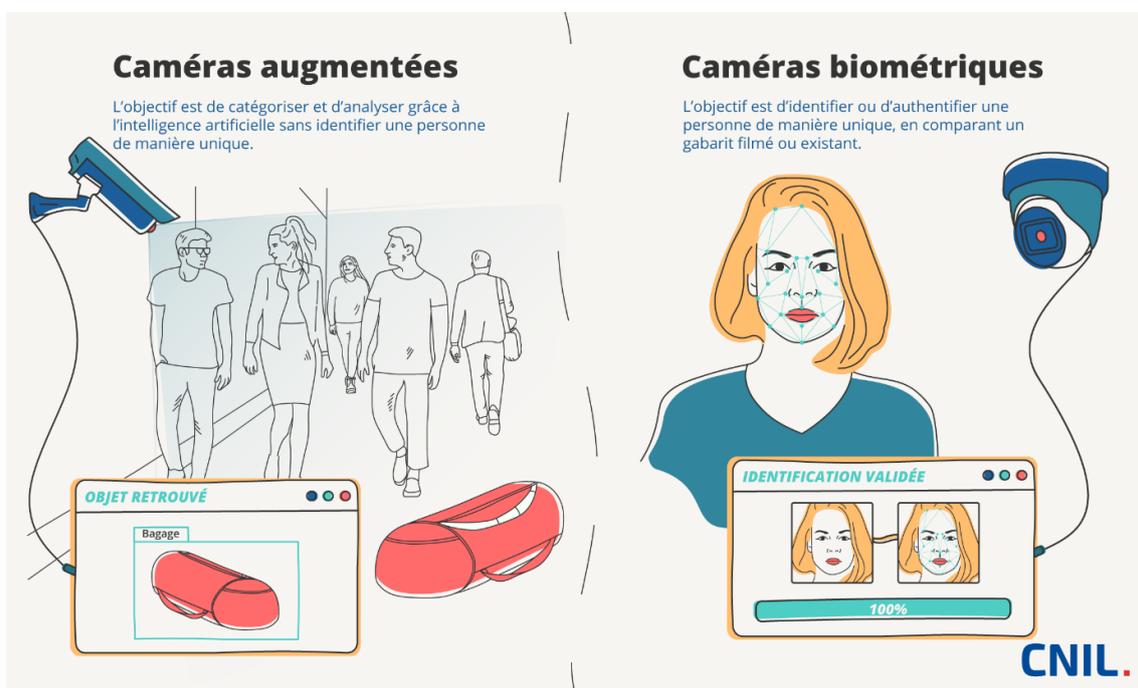
En définitive, le régime juridique expérimental mis en place pour les caméras « augmentées » est plutôt équilibré et il y a des garanties très solides pour le respect des droits fondamentaux. Ce régime juridique participe plus largement à la mise en oeuvre future du règlement européen sur l'IA puisqu'il détient des caractéristiques similaires, le droit français en matière d'IA peut donc apparaître comme un droit pionnier en la matière au niveau européen. Le développement d'un cadre juridique européen en matière d'intelligence artificielle va permettre de réguler les usages de cette technologie, notamment en matière de sécurité publique avec les caméras de vidéoprotection. En effet, la vidéo de manière générale « touchera à notre souveraineté, et donc à nos libertés »¹⁹³ surtout si elle s'accompagne d'intelligence artificielle comme la reconnaissance faciale, le cadre juridique qui sera mis en place au niveau européen est donc fondamental pour la souveraineté de l'Union européenne pour le développement d'intelligences artificielles éthiques et dignes de confiance.

Par conséquent, il est donc possible de conclure que le recours à l'intelligence artificielle en matière d'ordre public n'est pas une évolution technologique se faisant au détriment des libertés fondamentales en Occident.

¹⁹³ (R.) RIVATON, *Sourions, nous sommes filmés ! Pour un discours optimiste sur les caméras*, Paris, Éditions de l'Observatoire, coll. Alpha Essai, 2023, p. 243.

ANNEXES

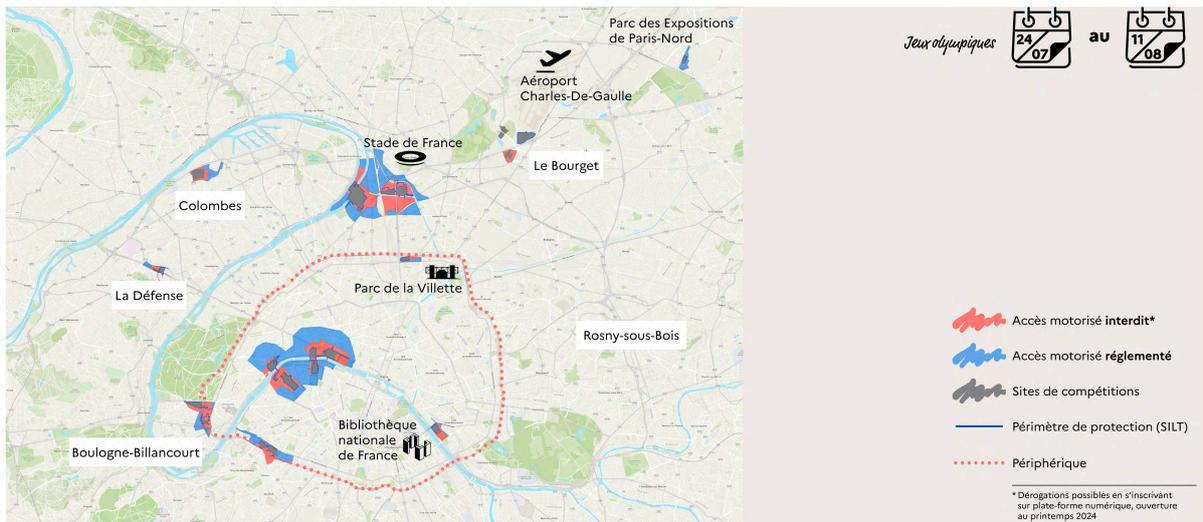
Annexe I : Synthèse des contributions concernant la consultation publique relative aux cameras intelligentes augmentées, établie par la CNIL en juillet 2022



Annexe II : Plan de sécurisation des sites olympiques issu du site internet de la Préfecture de police de Paris.

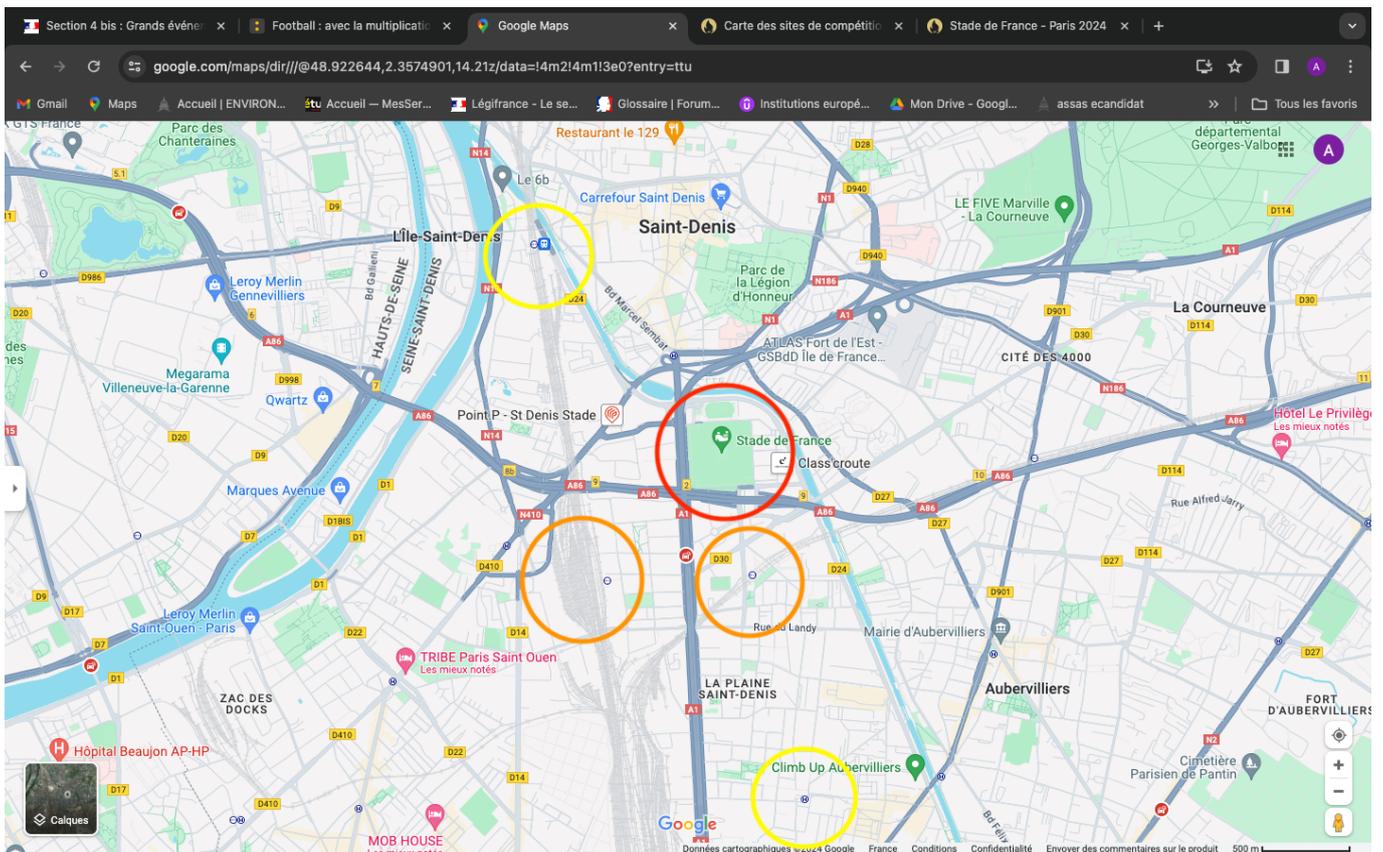

**MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER**
*Liberté
Égalité
Fraternité*


**PRÉFECTURE
DE POLICE**
*Liberté
Égalité
Fraternité*



Sites olympiques | Paris, petite couronne

Annexe III : Carte du site olympique du Stade de France comprenant les potentiels emplacements des caméras « augmentées »



Lieu de l'évènement sportif: Stade de France



Emprises de transports publics qui desservent le Stade de France



Emprises de transports publics conseillés par les organisateurs des Jeux Olympiques pour fluidifier les passages

Annexe IV : Panneaux d'information de la présence de caméras de vidéoprotection produits par la CNIL



VILLE PLACÉE SOUS VIDÉOPROTECTION

Ville placée sous vidéoprotection pour la sécurité des personnes et des biens. Les images sont conservées pendant un mois et peuvent être visionnées, en cas d'incident, par le centre de supervision urbain.

Pour exercer vos droits Informatique et Libertés, notamment votre droit d'accès aux images qui vous concernent, ou pour obtenir plus d'information sur ce dispositif, vous pouvez contacter notre délégué à la protection des données en écrivant à dpo@abcd.fr ou à l'adresse postale suivante : XXXX.

Pour en savoir plus sur la gestion de vos données personnelles et vos droits, rendez-vous sur le site de la commune – Rubrique « Politique de protection des données »

Vous pouvez introduire une réclamation auprès de la CNIL sur cnil.fr/plaintes



 **Non,**
cette information
n'est pas suffisante

 **Oui**

Annexe V : Exemple d'autorisation préfectorale de déploiement de caméras de vidéoprotection à Paris (06^e) en date du 19 février 2018, n° 20180136

Considérant les différents attentats intervenus depuis janvier 2015 et l'extrême gravité et l'importance des risques liés à la menace terroriste ;

Considérant la nécessité d'assurer, dans ces circonstances, la sécurité des personnes et des biens par des mesures adaptées à la gravité de la menace ;

Considérant que les risques particuliers d'atteinte à la sécurité des personnes et des biens et l'exposition particulière à un risque d'actes de terrorisme rendent nécessaire la mise en œuvre d'un système de vidéoprotection renforcé par l'ajout de caméras sur la voie publique à Paris ;

ARRETE

Article 1^{er} – Le directeur opérationnel des services techniques et logistiques est autorisé à procéder, dans les conditions ci-dessous, à l'installation d'un système de vidéoprotection de voie publique comportant 38 caméras implantées dans les voies du 6^e arrondissement de Paris (75006) fixées en annexe 1 du présent arrêté, pour une durée de cinq ans.

Article 2 – Ce dispositif de vidéoprotection a pour finalités :

- Sécurité des personnes ;
- Secours aux personnes, défense contre l'incendie, prévention des risques naturels ou technologiques ;
- Prévention des atteintes aux biens ;
- Protection des bâtiments publics ;
- Régulation du trafic routier ;
- Prévention d'actes de terrorisme ;
- Prévention du trafic de stupéfiants ;
- Constatation des infractions aux règles de la circulation.

Article 3 – Les enregistrements d'images sont conservés durant 30 jours et sont détruits à l'issue de ce délai.

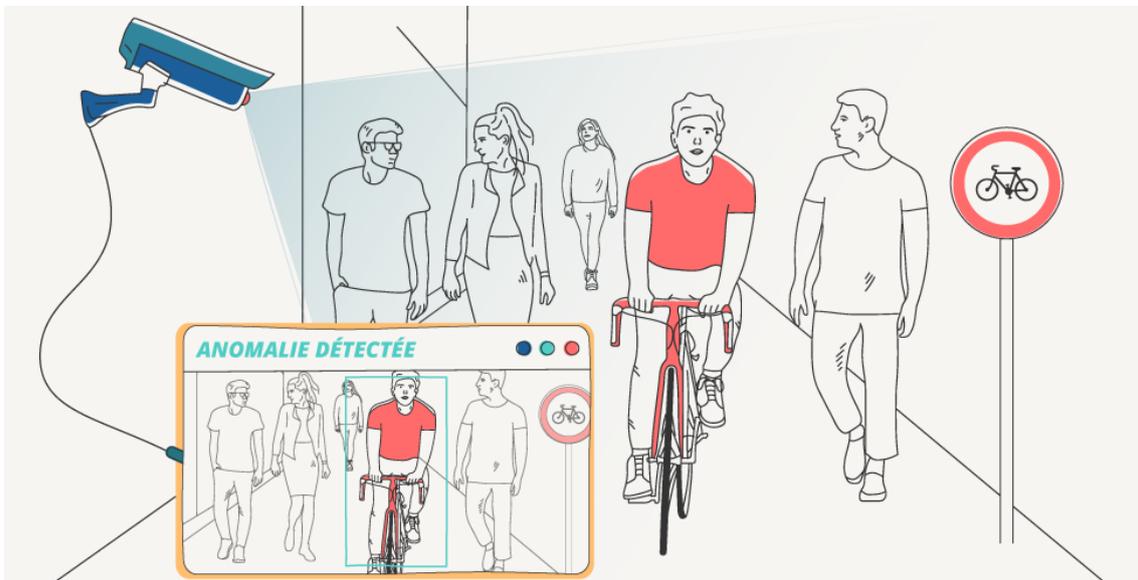
Article 4 – Le directeur opérationnel des services techniques et logistiques doit en particulier :

- Veiller à l'habilitation des personnes susceptibles d'exploiter et de visionner les images ;
- Procéder à l'information du public sur le dispositif mis en place et sur son responsable, de manière claire et permanente ;
- Mettre en œuvre un droit d'accès aux enregistrements ;
- Tenir un registre faisant apparaître les enregistrements réalisés, la date de destruction des images et celle de leur transmission éventuelle aux autorités judiciaires.

Le système ne doit pas permettre de visualiser les images de l'intérieur des immeubles d'habitation, ni celles de leurs entrées et les enregistrements ne peuvent être transmis à l'étranger.

Article 5 – I- Les fonctionnaires des services de police ou de gendarmerie nationales, ainsi que des douanes et des services d'incendie et de secours, dûment habilités et individuellement désignés à cet

Annexe VI : Illustration du rôle d'alerte des caméras « augmentées » produite par la CNIL

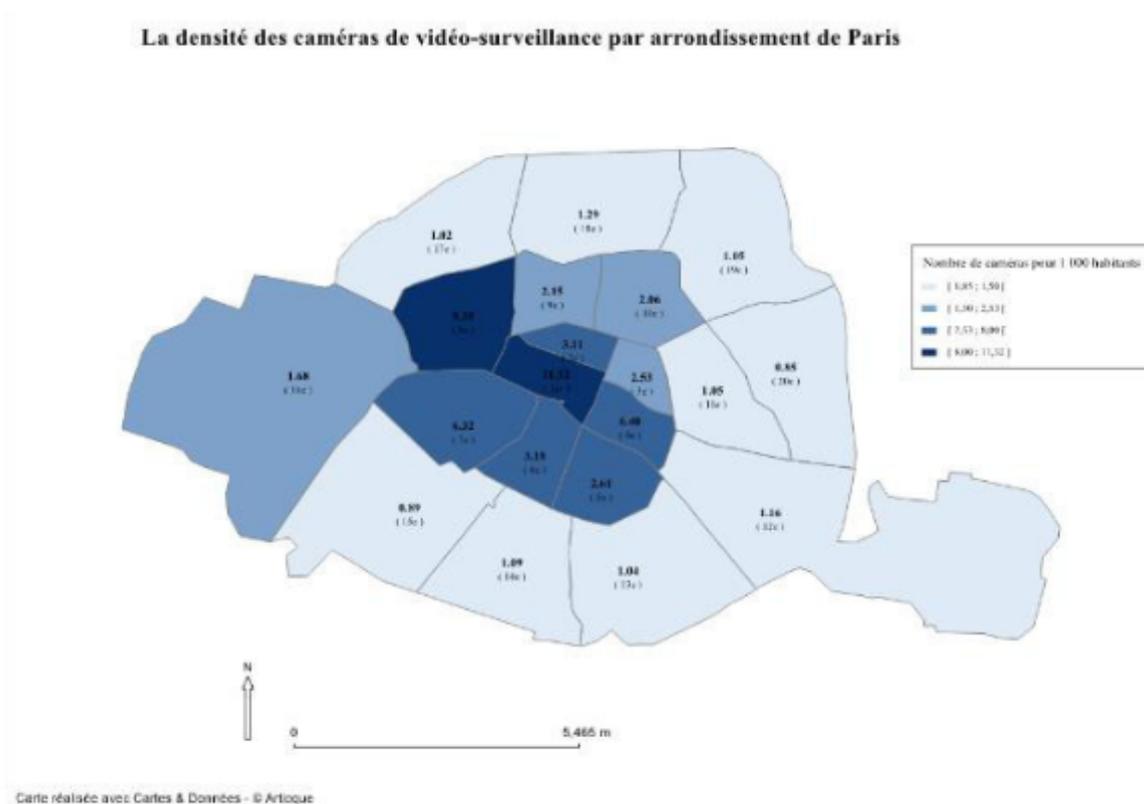


Annexe VII : Infographie sur les 25 critères de discrimination reconnus par la loi française.


MINISTÈRES
ÉDUCATION
JEUNESSE
SPORTS
ENSEIGNEMENT
SUPÉRIEUR
RECHERCHE
*Liberté
Égalité
Fraternité*



Annexe VIII : Cour des comptes, carte de la répartition des caméras de vidéoprotection par arrondissement de Paris, référé : le plan de vidéoprotection de la préfecture de police de Paris, 2 décembre 2021.



BIBLIOGRAPHIE

- Normes
 - Normes européennes

Charte des droits fondamentaux de l'Union européenne (2000/C 364/01) 18 décembre 2000.

Résolution législative du Parlement européen du 13 mars 2024 sur la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle, considérant n° 7.

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Directive (UE) 2016/680 du 27 avril 2016 dite « police-justice ».

- Normes constitutionnelles françaises

Loi constitutionnelle n° 2003-276 du 28 mars 2003 relative à l'organisation décentralisée de la République

- Normes législatives françaises

Loi n° 2023-380 du 19 mai 2023 *relative aux Jeux Olympiques et Paralympiques et portant diverses autres dispositions.*

Projet de loi n° 220 *relatif aux Jeux Olympiques et paralympiques 2024, 22 décembre 2022.*

Loi n° 2021-646 du 25 mai 2021 *pour une sécurité globale préservant les libertés.*

Ordonnance n° 2018-1125 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, du 12 décembre 2018.

Loi n° 2017-1510 du 30 octobre 2017 *renforçant la sécurité intérieure et la lutte contre le terrorisme.*

Loi n° 2016-1321 du 7 octobre 2016 *pour une République numérique.*

Loi n° 2011-267 du 14 mars 2011 *d'orientation et de programmation pour la performance de la sécurité intérieure.*

Loi n° 2010-1192 du 11 octobre 2010 *interdisant la dissimulation du visage dans l'espace public.*

Loi n° 2006-64 du 23 janvier 2006 *relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.*

Loi n° 2000-597 du 30 juin 2000 *relative au référé devant les juridictions administratives.*

Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés.*

Loi n° 70-643 du 17 juillet 1970 *tendant à renforcer la garantie des droits individuels des citoyens.*

- Normes réglementaires françaises

Arrêté n° 2024-00493 de la préfecture de police autorisant le recours aux caméras « augmentées » dans deux gares parisiennes afin de sécuriser le match de Football PSG-OL, 17 avril 2024.

Décret n° 2023-939 du 11 octobre 2023 relatif aux modalités de pilotage et d'évaluation de l'expérimentation de traitements algorithmiques d'images légalement collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs

Décret n° 2023-847 du 30 août 2023 portant application de l'article L. 211-11-1 du code de la sécurité intérieure aux « villages rugby » de la Coupe du monde de rugby 2023 et modifiant le décret du 22 décembre 2022 portant application de l'article L. 211-11-1 du code de la sécurité intérieure à la Coupe du monde de rugby 2023, JORF n°0202 du 1er septembre 2023.

Décret n° 2023-828 du 28 août 2023 relatif aux modalités de mise en œuvre des traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs, pris en application de l'article 10 de la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions.

Décret n° 2021-1397 du 27 octobre 2021 portant application de l'article L. 211-11-1 du code de la sécurité intérieure aux jeux Olympiques et Paralympiques de 2024.

Décret-loi du 23 octobre 1935 portant réglementation des mesures relatives au renforcement du maintien de l'ordre public.

- Ouvrages

BAUER (A.) et FREYNET (F.), *vidéosurveillance et vidéoprotection*, Paris, PUF, coll. Que sais-je ?, 2008, 128 p.

CAZENEUVE (B.) et FARDE (G.), *La lutte antiterroriste*, Paris, PUF, coll. Savoirs, 2023, 256 p.

FAVOREU (L.), DUFFY-MEUNIER (A.), FASSASSI (I.), GAÏA (P.), LE BOT (O.), PECH (L.), PENA (A.), ROUX (A.) & SCOFFONI (G.), *Droit des libertés fondamentales*, Dalloz, coll. Précis, 8e édition, 2021, 720 p.

HUGO (V.), *Le dernier jour d'un condamné*, Classiques, édition Pocket, 94 p.

RIVATON (R.), *Sourions, nous sommes filmés ! Pour un discours optimiste sur les caméras*, Paris, Éditions de l'Observatoire, coll. Alpha Essai, 2023, 256 p.

RIVERO (J.), *Libertés publiques*, Montchrestien, 1989, 296 p.

FAUVARQUE-COSSON (B.) et HAZARD-TOURILLON (A.-M.) (dir.), *Droit & Grands Enjeux du Monde Contemporain*, Turin, Nathan, 2021, 265 p.

- Articles

ALVES (C.-M.), BOFFA (R.), CIROTTEAU (M.), GOHIN (O.), GRANGER (M.-A.), LEGENDRE (C.), MARCHADIER (F.) et MATTIUSI (J.), « Les Jeux olympiques et paralympiques et le droit », *Revue d'Assas*, n° 27, mars 2024.

CASTETS-RENARD (C.) et TURCI (A.), « 'Caméras augmentées' : un danger pour les libertés lors des Jeux Olympiques et Paralympiques (et au-delà) ? », *Recueil Dalloz*, numéro 22, 2023.

DEBOVE (F.), « Surveiller et punir dans un monde 3.0 », *AJPénal*, Dalloz, Chronique de déontologie de la sécurité n°3, n° 202203, mars 2022.

DESMURAUX (M.), « La SNCF et la RATP autorisées à expérimenter la vidéosurveillance "intelligente" à Paris entre le 19 et le 22 avril 2024 », *AEF Info*, n° 710927, 17 avril 2024.

DUTHEILLET DE LAMOTHE (L.) et JANICOT (T.), « Les expérimentations : comment innover dans la conduite des politiques publiques », *AJDA*, Dalloz, n° 35/2019, 21 octobre 2019.

EGEA (A.), TAÏEB (L.), PELLAN (B.) et GOLDBERG (G.), « Actualité Informatique et libertés », Dalloz, *AJDA*, n° 9/2023, 13 mars 2023.

FAUVEL (L.), REVOL (S.) et HURNIC (M.-E.), « 'Caméras « intelligentes' : sécuriser leur conformité au RGPD », *Revue Lamy Droit de l'Immatériel*, No 200, 1er février 2023.

FILLIEULE (O.), « Stratégies de la rue », Paris, *Presses de Sciences Po*, 1997, 440 p.

GALATAS (I.) et MARS (J.), « Paris 2024 : cérémonie d'ouverture des Jeux olympiques – Innovante ? Oui ! Sécurisée (CBRNe/NBCe) ? Non ! », *ESKA*, in *Sécurité globale* 2022/4, n° 32, 2022.

HAAS (G.) et ASTIER (S.), « Les biais de l'intelligence artificielle : quels enjeux juridiques ? », Dalloz, *Répertoire IP/IT et Communication*, Juillet 2019.

LASSERRE (V.), *Répertoire de droit civil, Loi et règlement, Naissance des lois et des règlements*, Juillet 2015 (actualisation : Janvier 2016).

LEQUESNE ROTH (C.), « Mise en demeure de Clearview AI par la CNIL : les jalons d'un combat pour le droit à l'anonymat », *Dalloz, IP/IT* 2022. 220.

MAZEAUD (V.), « La constitutionnalisation du droit au respect de la vie privée », *NCCC* n°48 (dossier : vie privée), juin 2015.

PORTALIS (J.-É.-M.), Discours préliminaire sur le projet de Code civil, 1er Pluviôse an IX (21 janvier 1801).

SERUGA-CAU (E.), « L'utilisation de « *caméras augmentées* » dans l'espace public ou comment innover sans (trop) surveiller », *Communication - Commerce électronique*, Lexisnexis, n° 78, juillet-août 2023.

STAHL (J.-H.), « L'expérimentation en droit français : une curiosité en mal d'acclimatation », *Revue juridique de l'économie publique* n° 681, 2010, étude 11.

- Jurisprudences

- Décisions de la Cour européenne des droits de l'homme

CEDH, 28 janvier 2003, n° 44647/ 98, *Peck c. Royaume-Uni*.

- Décisions de la Cour de Justice de l'Union européenne

CJUE, 11 décembre 2014, C-212/13.

- Décisions du Conseil constitutionnel

Cons. const., 17 mai 2023, n° 2023-850 DC, *Loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions*.

Cons. const., 1er décembre 2017, n° 2017-677 QPC, *Ligue des droits de l'Homme [Contrôles d'identité, fouilles de bagages et visites de véhicules dans le cadre de l'état d'urgence]*.

Cons. const., n° 2012-652 DC, 22 mars 2012, *Loi relative à la protection de l'identité*.

Cons. const., 16 juillet 2009, n° 2009-584 DC, *Loi portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires.*

Cons. const., 12 août 2004, n° 2004-503 DC, *Loi relative aux libertés et responsabilités locales.*

Cons. const., 23 juillet 1999, n° 99-416 DC, *Loi portant création d'une couverture maladie universelle.*

Cons. const., 18 janvier 1995, n° 94-352 DC, *Loi d'orientation et de programmation relative à la sécurité.*

Cons. const., 28 juillet 1993, n° 93-322 DC, *Loi relative aux établissements publics à caractère scientifique, culturel et professionnel.*

Cons. const., 27 juillet 1982, n° 82-141 DC, *Loi sur la communication audiovisuelle.*

- Décisions du Conseil d'État

Conseil d'État, ordonnance de référé, 21 décembre 2023, n° 489990.

Conseil d'État, ordonnance de référé, 18 mai 2020, n° 440442.

Conseil d'État, ordonnance de référé, 25 octobre 2007, n° 310125.

Conseil d'État, Ass., 27 octobre 1995, n° 13672, *Commune de Morsang-sur-Orge.*

- Décisions de la Cour de cassation

Cour de cassation, Première chambre civile, 13 septembre 2017, 16-22.967, Publié au bulletin.

Cour de cassation, Chambre criminelle, 9 février 2016, n° 14-82.234.

- Décisions de tribunal administratif

Tribunal administratif de Lille, ordonnance de référé, n° 2310103 et 2310163, 29 novembre 2023.

Tribunal administratif de Nice, ordonnance de référé, n° 2305692, 2306593 et 2305712, 23 novembre 2023.

Tribunal administratif de Caen, ordonnance de référé, n° 2303004 et 2303012, 22 novembre 2023.

- Rapports administratifs

Comité VEIL (S.), Rapport au Président de la République : « Redécouvrir le Préambule de la Constitution », 17 décembre 2008, 209 p.

Défenseur des droits, Rapport « Algorithmes : prévenir l'automatisation des discriminations », 2020.

- Rapports du Sénat

Sénat, Rapport d'information n° 527 fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur l'application de la loi du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, par les sénateurs CANAYER (A.) et de LA GONTRIE (M.-P.), 10 avril 2024, 148 p.

Sénat, Rapport n° 248 fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le projet de loi relatif aux jeux Olympiques et Paralympiques de 2024, par le sénateur CANAYER (A.), 18 janvier 2023, 119 p.

Sénat, Rapport d'information n° 627 fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles, par les sénateurs DAUBRESSE (M.-P.) BELENET (A.) et DURAIN (J.), 10 mai 2022.

- Rapports de l'Assemblée nationale

Assemblée nationale, Rapport d'information n° 1089 sur les enjeux de l'utilisation d'images de sécurité dans le domaine public dans une finalité de lutte contre l'insécurité, (P.) GOSSELIN et (P.) LATOMBE, 12 avril 2024, 152 p.

Assemblée nationale, Rapport n° 939 fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, sur le projet de loi, adopté par le Sénat après engagement de la procédure accélérée, relatif aux jeux Olympiques et Paralympiques de 2024, et portant diverses autres dispositions, fait par le député VUILLETET (G.), 9 mars 2023, 468 p.

- Avis consultatifs du Conseil d'État

Conseil d'État, étude d'impact sur le projet de loi relatif aux jeux Olympiques et Paralympiques de 2024, 20 décembre 2022, 177 p.

Conseil d'État, n° 406383, avis relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, 15 décembre 2022, 18 p.

Conseil d'État, étude à la demande du Premier ministre « Intelligence artificielle et action publique : construire la confiance, servir la performance », étude adoptée en assemblée générale plénière du 31 mars 2022, 360 p.

Conseil d'État, n° 393744, avis consultatif portant sur le projet de loi pour un état au service d'une société de confiance, 27 novembre 2017.

Conseil d'État, n° 393348, avis sur un projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme, 15 juin 2017, 10 p.

- Avis consultatifs de la CNIL

CNIL position sur les conditions de déploiement des caméras dites « intelligentes » ou « augmentées » dans les espaces publics, juillet 2022.

CNIL délibération n° 2022-043 du 14 avril 2022 portant avis sur un projet de décret relatif à l'extension des destinataires d'images de vidéoprotection.

- Sites Internet

Briefcam : Vidéo du filtre *Line crossing* : <https://www.briefcam.com/resources/videos/detecting-traffic-violations-with-briefcam/> (consulté le 24 avril 2024).

CEDH : Tableau statistique <https://www.echr.coe.int/documents/d/echr/stats-violation-2023-fra>

CNIL :

- Affaire Clearview AI : <https://www.cnil.fr/fr/reconnaissance-faciale-sanction-de-20-millions-deuros-lencontre-de-clearview-ai> (consulté le 09 avril 2024).
- Rubrique « missions » : <https://cnil.fr/fr/la-cnil/les-missions-de-la-cnil> (consulté le 18 avril 2024).
- Définition de l'intelligence artificielle : <https://www.cnil.fr/fr/definition/intelligence-artificielle#:~:text=L'intelligence%20artificielle%20est%20un,r%C3%A9aliser%20des%20t%C3%A2ches%20bien%20d%C3%A9finies> (consulté le 1er avril 2024).
- Définition de la *smart city* : <https://www.cnil.fr/fr/definition/smart-city>.
- Droit d'information pour les personnes filmées : <https://www.cnil.fr/fr/la-videosurveillance-videoprotection-sur-la-voie-publique> (consulté le 13 avril 2024).

Colloque MBA Management de la sécurité du 29 février 2024, Sécuriser l'évènement : l'IA est-elle la martingale absolue ? : <https://www.youtube.com/watch?v=N46xZEa0-ds>

DGSI : <https://www.dgsi.interieur.gouv.fr/la-dgsi-a-vos-cotes/lutte-contre-terrorisme/letat-de-la-menace-terroriste-en-france>

FranceInfo : https://www.francetvinfo.fr/sports/foot/football-avec-la-multiplication-recente-des-violences-hors-des-stades-le-hooliganisme-resurgit-il-pour-autant-en-france_5450203.html

La Boussole : <https://laboussole.coop/2021/01/05/recueil-de-citations-sur-les-themes-de-la-surveillance-et-de-lintime/>

La Quadrature du Net : <https://www.laquadrature.net/biometrie-jo/>

Le Figaro : <https://www.lefigaro.fr/actualite-france/jo-paris-2024-cameras-intelligentes-concert-depeche-mode-bercy-20240216>

Les Numériques : <https://www.lesnumeriques.com/societe-numerique/tiktok-lite-mise-en-pause-du-systeme-de-remuneration-en-europe-n221091.html>

Paris 2024 : <https://www.paris2024.org/fr/site/stade-de-france/>

Radio France : <https://www.radiofrance.fr/franceculture/le-panoptique-a-l-origine-de-la-societe-de-surveillance-8706244>

Wintics, page collectivités : <https://wintics.com/collectivites/> (consulté le 23 avril 2024).

20 Minutes : <https://www.20minutes.fr/nice/1854995-20160530-nice-estrosi-ciotti-ecrivent-valls-autoriser-reconnaissance-faciale>

Table des matières

| | |
|--|----|
| REMERCIEMENTS | 2 |
| TABLE DES ABRÉVIATIONS | 3 |
| SOMMAIRE..... | 4 |
| INTRODUCTION GÉNÉRALE..... | 5 |
| TITRE I : LE RECOURS EXPÉRIMENTAL AUX CAMÉRAS « AUGMENTÉES » ET LE RENOUVELLEMENT DE LA QUESTION DE LA PROTECTION DE LA VIE PRIVÉE..... | 10 |
| Chapitre 1 : Le cadre juridique de l'article 10 de la loi du 19 mai 2023 concernant le déploiement des caméras « augmentées »..... | 12 |
| Section 1 : L'utilisation des caméras « augmentées » pour lutter contre les atteintes les plus graves à l'ordre public | 12 |
| Paragraphe 1 : Le recours aux caméras « augmentées » afin de sécuriser les « manifestations » sportives, récréatives et culturelles..... | 13 |
| A. La limite matérielle de l'expérimentation des caméras « augmentées aux seules « manifestations » sportives, récréatives et culturelles | 13 |
| B. Le recours aux caméras « augmentées » pour prévenir les atteintes les plus graves à l'ordre public | 15 |
| Paragraphe 2 : La qualification de « grand évènement » des jeux Olympiques permettant d'étendre le périmètre géographique de déploiement des caméras « augmentées » | 17 |
| A. Le recours aux caméras « augmentées » pour sécuriser les lieux connexes à l'évènement susceptible de faire l'objet d'un acte de terrorisme..... | 17 |
| B. Le déploiement des caméras « augmentées » dans les lieux publics desservant le lieu de l'évènement | 19 |
| Section 2 : Les limites tenant à l'usage des caméras « augmentées » | 20 |
| Paragraphe 1 : L'encadrement juridique des normes expérimentales | 21 |
| A. La limite formelle à l'expérimentation du recours aux caméras « augmentées » | 21 |
| B. La limitation temporelle de cette expérimentation..... | 23 |
| Paragraphe 2 : Les limites relatives à la conception et l'utilisation des caméras « augmentées » | 26 |
| A. L'absence textuelle de recours aux données biométriques et à la reconnaissance faciale | 26 |

| | |
|---|-----------|
| B. La fonction d’alerte des caméras « augmentées » | 29 |
| Chapitre 2 : Les nécessaires garanties de protection de la vie privée lors du recours des caméras « augmentées » | 31 |
| Section 1 : La définition de la notion de droit au respect de la vie privée | 31 |
| Paragraphe 1 : La protection composite du droit au respect de la vie privée | 32 |
| A. La jurisprudence du Conseil constitutionnel concernant la protection du droit au respect de la vie privée | 33 |
| B. La protection internationale du droit au respect de la vie privée | 35 |
| Paragraphe 2 : L’application du droit au respect de la vie privée aux caméras intelligentes | 37 |
| A. Le respect du droit à l’anonymat des personnes soumises aux caméras « augmentées » | 37 |
| B. Les composants numériques du droit au respect de la vie privée soumis aux caméras « augmentées » | 40 |
| Section 2 : La vidéoprotection intelligente, un outil de police administrative | 43 |
| Paragraphe 1 : Le nécessaire arrêté préfectoral autorisant le déploiement des caméras « augmentées » | 44 |
| A. L’insuffisante référence générale à la lutte antiterroriste pour justifier l’utilisation des caméras « augmentées » | 45 |
| B. Le recours aux caméras « augmentées » limité à la durée de l’évènement à sécuriser | 48 |
| Paragraphe 2 : La garantie de l’accès au juge pour contester l’utilisation des caméras « augmentées » | 49 |
| A. Les différents recours possibles devant le juge administratif contre l’usage des caméras « augmentées » | 50 |
| B. L’exemple des contentieux Briefcam | 52 |
| TITRE II : LE RENFORCEMENT DU CONTRÔLE NON JURIDICTIONNEL DES SYSTÈMES DE VIDÉOPROTECTION ET L’ÉLABORATION D’UNE RÉGLEMENTATION RELATIVE À L’INTELLIGENCE ARTIFICIELLE | 54 |
| Chapitre 1 : L’expérimentation des caméras « augmentées » mettant en valeur cette technologie et le rôle de la CNIL | 56 |

| | |
|---|----|
| Section 1 : Une appréhension technique de l'intelligence artificielle au travers des caméras « augmentées » | 57 |
| Paragraphe 1 : La détection de situations anormales par les caméras « augmentées » | 58 |
| Paragraphe 2 : Le développement du traitement algorithmique pour l'expérimentation des caméras « augmentées » au travers de l'utilisation des données | 59 |
| Section 2 : Le rôle central de la CNIL dans le contrôle des systèmes de vidéoprotection | 61 |
| Paragraphe 1 : L'unification des régimes juridiques de la vidéoprotection au profit de leur soumission au droit des données à caractère personnel..... | 61 |
| Paragraphe 2 : Le rôle de la CNIL dans l'évaluation de l'expérimentation des caméras « augmentées » | 63 |
| Chapitre 2 : Vers une réglementation de l'intelligence artificielle au niveau européen | 65 |
| Section 1 : L'établissement de lignes rouges dans l'utilisation de l'intelligence artificielle..... | 66 |
| Paragraphe 1 : L'interdiction de classer socialement les personnes | 67 |
| Paragraphe 2 : Les différentes finalités possibles pour le recours à l'intelligence artificielle | 69 |
| Section 2 : L'établissement d'un cadre juridique « digne de confiance » | 71 |
| Paragraphe 1 : Les principes généraux du règlement européen sur l'intelligence artificielle relatifs à la personne humaine | 71 |
| Paragraphe 2 : Les principes généraux du règlement européen ayant pour objet central l'intelligence artificielle..... | 72 |
| CONCLUSION | 73 |
| ANNEXES | 75 |
| BIBLIOGRAPHIE | 83 |

RÉSUMÉ :

Les Jeux Olympiques et Paralympiques 2024 de Paris seront l'occasion d'expérimenter les caméras « augmentées ». Il s'agit d'une technologie reposant sur l'intelligence artificielle pour traiter en temps réel les images captées par les caméras de vidéoprotection dans le but de détecter des événements prédéterminés.

À première vue, cette technologie rappelle le « télécran » décrit dans *1984*, toutefois elle s'en écarte grandement de par sa finalité de protection de l'ordre public lors de grands événements. Néanmoins, cette technologie porte atteinte au droit au respect de la vie privée en analysant en temps réel les personnes filmées, la loi apporte donc différentes garanties pour protéger ce droit. Selon l'interprétation de la loi retenue, ces caméras pourront être déployées dans une zone plus ou moins étendue.

Une autre question intéressante pour ce sujet porte sur l'intelligence artificielle en tant que technologie. En effet, le droit commence à appréhender cette technologie afin d'en limiter les usages et éviter les dérives comme en Chine avec le crédit social. C'est dans cette optique que l'Union européenne a adopté une proposition de règlement sur l'intelligence artificielle, laquelle proposition établit une distinction selon le degré de risques causés par l'intelligence artificielle sur les droits fondamentaux. Cette future réglementation prévoit également des lignes rouges à ne pas franchir pour que le système d'intelligence artificielle puisse être conçu, développé et mis sur le marché européen. Afin de respecter ces lignes rouges, le règlement prévoit également des principes fondamentaux s'imposant aux intelligences artificielles.

Mots clés : Caméras « augmentées » / Expérimentation / Protection de la vie privée / Données personnelles / Intelligence artificielle / Vidéoprotection / Vidéoprotection intelligente

SUMMARY :

The Olympics and Paralympics Games of 2024 in Paris will be the occasion to trial some new technologies : smart surveillance camera. This is a new technology based on artificial intelligence, it will process all images coming from the surveillance camera in real time in order to spot some predetermined events.

At first sight, this technology can be referred as the 'telescreen' from 1984, nevertheless its only purpose is to protect public order against serious danger during big events like the Olympics Games.

Nonetheless, this technology has an impact on the right to privacy because it will analyze people all the day long, therefore the law came with safeguards to protect this right. According to the reading of the law, the area of deployment of this technology can be quite big because other legal regime can be incorporated in this experiment.

Another interesting question is related directly to the artificial intelligence itself. Indeed, the law system has started to take into account this technology in order to prevent some wrong use of it as in China with the scoring social system. Therefore, the European Union has just approved a bill regarding artificial intelligence that will be applied from 2026. This bill will protect fundamental rights according to the fundamental principles of the European Union. First, this bill incorporated some limits to the use of artificial intelligence based on the dangerousness of them regarding fundamental rights. Then, this bill has built some fundamental principles related to the development and the marketing authorization of the artificial intelligence. This bill is the first one to control the use of artificial intelligence in the world.

Key words : Smart surveillance camera / Trial / Respect for the right to private life / Personal data / Artificial intelligence / Security camera system / Intelligent security camera system