LE COURRIER DES MAIRES
et des élus locaux

Intelligence artificielle et vidéosurveillance : entre controverses et défis juridiques

Publié le 02/10/2024 à 10h00

© Adobe stock

L'intégration de l'intelligence artificielle dans les dispositifs de vidéoprotection se heurte à l'absence d'un cadre juridique adapté. Toutefois, des initiatives législatives et réglementaires récentes laissent entrevoir des perspectives d'évolutions. C'est dans ce contexte que des procédures en référé liberté ont été engagées en novembre 2023 à l'encontre de collectivités concernant le recours à ce type de caméras dit caméras « augmentées ».
Retour sur l'évolution du cadre juridique applicable à ces dispositifs, à l'heure où leur utilisation par des communes fait l'objet de recours contentieux.

Par David Conerardy, avocat à la cour, et Coralie Estanol, stagiaire, cabinet Seban et associés

La loi du 21 janvier 1995 d'orientation et de programmation relative à la sécurité fixe, dans son article 10, le premier cadre juridique en matière de vidéosurveillance (devenue vidéoprotection) sur la voie publique et dans les lieux ouverts au public. Désormais, avec l'avènement de l'intelligence artificielle de nouveaux types de caméras, dites « augmentées » et « biométriques », voient le jour. Ces dispositifs, qui sont « *constitués de logiciels de traitements automatisés d'images associés à des caméras »,* permettant « *d'extraire diverses informations à partir de flux vidéo qui en sont issus* »[1], posent de nouvelles problématiques éthiques, politiques et juridiques. En effet, comme le souligne le Conseil d'État dans le cadre

de son étude annuelle de 2014, l'ambivalence du phénomène numérique réside dans le fait qu'il « *ouvre de nouveaux espaces de libertés, tout en étant porteur de risques pour celles-ci* »[2]. Toutefois, l'atteinte qui est portée aux droits et libertés des individus doit toujours être strictement proportionnelle, nécessaire et appropriée à la finalité poursuivie. La mise en œuvre de ces caméras, couplées à des systèmes d'intelligence artificielle, doit donc être associée à des garanties juridiques fortes.

Cependant, au regard du décalage de potentialité et de performance induit par ces technologies, le cadre juridique habituellement adapté à la vidéoprotection traditionnelle s'avère difficilement transposable. Ainsi, le recours aux caméras augmentées se heurte à un flou juridique, tandis que les caméras biométriques font l'objet d'une interdiction par principe, à l'exception de certains cas très spécifiques.

C'est dans ce contexte que, le 14 novembre 2023, le journal Disclose a fait état de l'utilisation, depuis 2015, par les forces de l'ordre du logiciel d'analyse d'images de vidéoprotection de la société israélienne Briefcam[3]. En effet, l'article révèle que plus d'une centaine de communes auraient équipé leurs polices municipales de cette technologie. Ces caméras dites « augmentées » seraient dotées de diverses fonctionnalités qui comporteraient un risque pour les droits et libertés des individus. À la suite de cette déclaration, la Commission nationale informatique et libertés (Cnil) a annoncé initier une procédure de contrôle concernant le recours à ces dispositifs par les collectivités.

1- Les défis juridiques induits par l'émergence de caméras dotées d'intelligence artificielle

Alors que la Cnil a pris position sur les caméras augmentées, ouvrant ainsi la voie à de nouvelles possibilités d'expérimentation, il est envisageable que cette position évolue avec l'entrée en vigueur du Règlement sur l'intelligence artificielle.

Un encadrement juridique lacunaire dans l'attente d'une clarification

En France, le domaine de la vidéoprotection est régi par le code de la sécurité intérieure et le RGPD. Cependant, la Cnil considère qu'en raison de leur différence de potentialité, les caméras dotées d'intelligence artificielle font peser de nouveaux risques sur les droits et libertés individuelles et ne peuvent donc pas être assimilées aux dispositifs de vidéoprotection traditionnels. Ainsi, dans sa position de 2022 intitulée « *Caméras dites 'intelligentes' ou 'augmentées' dans les espaces publics* », la Cnil déclare que le code de la sécurité intérieure n'est pas transposable à ces nouvelles technologies. Néanmoins, elle précise qu'il n'interdit pas pour autant leur déploiement[4].

De plus, la Cnil opère une distinction entre les caméras dites « augmentées » et les caméras biométriques. À cet égard, elle juge que si toutes deux recourent à l'intelligence artificielle, les premières, contrairement aux secondes, n'ont pas pour objectif d'identifier de manière unique une personne au moyen du traitement de données biométriques.

Partant, au regard des données sensibles qu'elles traitent, conformément aux articles 9 du RGPD[5] et 10 de la directive Police justice[6], sauf exceptions, l'usage des caméras biométriques est en principe interdit[7].

Concernant les caméras « *augmentées* », la Cnil souligne l'applicabilité de la réglementation sur la protection des données. À cet effet, elle insiste sur la nécessité de respecter les principes fondamentaux posés par la loi informatique et libertés, qui transpose notamment la directive police justice, et par le RGPD dans leur mise en œuvre. Elle n'établit pas une base légale spécifique sur laquelle devrait s'appuyer ce type de traitement, mais recommande une analyse au cas par cas conformément à l'article 6 du RGPD. Elle préconise également la réalisation d'une analyse d'impact (AIPD), et pour une large majorité des cas d'usage, en amont de la réalisation du traitement. Par ailleurs, lorsque les personnes concernées par un traitement de données sont privées de leur droit d'opposition, la Cnil rappelle qu'en vertu de l'article 23 du RGPD, la mise en œuvre d'un tel traitement devra alors être autorisée par un cadre juridique spécifique, de nature a minima réglementaire.

Enfin, la Cnil ouvre une brèche au législateur en précisant que le recours à ce type de technologie, à des fins de police administrative générale ou de police judiciaire, semble devoir être subordonnée à l'existence d'un encadrement législatif spécifique au regard de l'article 34 de la Constitution.

Les perspectives d'évolution

Le gouvernement, dans le cadre de sa stratégie nationale de prévention de la délinquance pour 2020-2024, a manifesté son intention « *d'expérimenter le traitement automatisé de l'image, dans le respect des libertés individuelles* » en matière de vidéoprotection (mesure n° 26)[8]. La concrétisation de cette volonté s'est notamment matérialisée en 2023 au travers de la loi relative aux Jeux Olympiques et Paralympiques[9], qui établit le premier cadre expérimental légal pour l'utilisation des caméras « augmentées »[10]. En effet, l'article 10 de cette loi autorise l'analyse « en temps réel » des images captées par ces caméras pour assurer la sécurité d'activités récréatives, culturelles ou sportives lors des Jeux olympiques. En accord avec les recommandations de la Cnil de juillet 2022, des garanties substantielles ont été prévues dans la loi « JOP ». En effet, le traitement de données opérées par ces caméras est légalement fondé sur une loi et un décret[11], pris après avis de la Cnil. L'article 14 du décret n° 2023-828 du 28 août 2023 prévoit notamment que tout traitement, non inclus dans l'analyse d'impact cadre transmise par le ministère de l'intérieur à la Cnil, doit également faire l'objet d'une telle analyse. De plus, des mesures de contrôle humain et un système de gestion des risques ont été instaurés et tout traitement biométrique est proscrit. Par ailleurs, l'emploi du traitement algorithmique est conditionné à la délivrance par le représentant de l'Etat dans le département ou, à Paris, par le préfet de police, d'une autorisation devant être renouvelée mensuellement.

De plus, bien que la loi relative aux Jeux Olympiques et Paralympiques de 2023 exige une information générale du public concernant l'emploi de traitements algorithmiques sur les images collectées, cette obligation peut être écartée dans certaines circonstances (art. 10) de la loi JOP. Dans les cas où une telle information n'est pas prodiguée, la possibilité d'exercer ses droits en matière de données personnelles est de fait restreinte[12]. Par ailleurs, l'application temporelle de cette expérimentation, couvrant la période des Jeux Olympiques et au-delà (de la promulgation de la loi jusqu'au 31 mars 2025), a suscité des réserves, ce qui a notamment conduit à une saisine du Conseil constitutionnel.

Par sa décision n° 2023-850 DC du 17 mai 2023, celui-ci a jugé que l'utilisation des caméras « augmentées », compte tenu des garanties mises en œuvre, ne méconnaissait pas le droit au respect de la vie privée. Cependant, une réserve d'interprétation a été imposée, exigeant que le préfet mette fin immédiatement à une autorisation d'utilisation du traitement algorithmique si les conditions initiales, justifiant sa délivrance, ne sont plus réunies[13]. Il conviendra de voir de quelle manière, dans la pratique, la conciliation de cette exigence avec les impératifs de sécurité s'articulera.

Enfin, la loi prévoit également la remise d'un rapport d'évaluation, le 31 décembre 2024, en vue d'une éventuelle pérennisation par le législateur du dispositif, avec la possibilité d'ajuster ses modalités de mise en œuvre et son champ d'application[14].

Parallèlement, l'encadrement juridique des caméras couplées à des systèmes d'intelligence artificielle est voué à évoluer avec l'entrée en vigueur du Règlement européen sur l'intelligence artificielle. Le projet de ce Règlement interdit, par principe, l'usage à des fins répressives de systèmes d'identification biométrique à distance en temps réel dans un espace ouvert au public, tout en prévoyant des dérogations strictement encadrées[15]. Cependant, dans leur avis conjoint du 18 juin 2021[16], le Contrôleur européen à la protection des données ainsi que le Comité européen de la protection des données, jugeant les garanties prévues insuffisantes, ont recommandé une interdiction totale du recours à l'intelligence artificielle en vue d'une reconnaissance automatisée des caractéristiques humaines dans les espaces accessibles au public[17].

Tandis que le cadre juridique des caméras dotées d'intelligence artificielle semble se dessiner peu à peu, certaines communes font l'objet de procédures judiciaires en raison du recours à ces dispositifs.

2- L'usage controversé du logiciel de la société Briefcam par des communes

L'utilisation du logiciel de la société Briefcam par des communes a été contestée dans une série de procédures en référé-liberté. Si, dans la première décision rendue, le juge a considéré que le recours à ce logiciel nécessitait qu'une mesure de sauvegarde, de nature à stopper l'atteinte au droit au respect de la vie privée, soit prise, les décisions rendues par la suite ont démontré, qu'en l'absence du recours à de nombreuses fonctionnalités du dit logiciel, de telle mesure n'étaient pas justifiées.

Le recours aux caméras intelligentes…

À la suite des révélations du journal Disclose concernant le recours par certaines communes au logiciel de la société Briefcam, des associations et des syndicats, notamment, ont engagé, en novembre 2023, plusieurs procédures de référés libertés. Le 22 novembre 2023[18] le tribunal administratif de Caen a été le premier à se prononcer sur le sujet, concernant l'utilisation du logiciel de la société Briefcam par la Communauté de commune de Cœur Côte Fleurie.

Dans un premier temps, le juge reconnaît que le droit au respect de la vie privée, incluant le droit à la protection des données personnelles, constitue une liberté fondamentale au sens de l'article L. 521-2 du code de justice administrative. Il affirme ensuite que le dispositif de surveillance relève du champ d'application de la directive dite Police Justice du 27 avril

2016[19], transposée en droit interne au titre 3 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Partant, le juge a relevé plusieurs manquements à la réglementation en matière de données personnelles. Tout d'abord, il a considéré que le traitement de données était dépourvu de base légale puisque ce type de traitement doit être prévu et encadré par la loi ou un acte réglementaire, ce qui n'était pas le cas en l'espèce. Ensuite, le juge estime qu'en permettant l'identification de personnes sur la base de leurs caractéristiques propres, le système portait « *une atteinte grave et manifestement illégale au respect de la vie privée* ». Ainsi, en l'absence de démonstration que des moyens moins intrusifs n'auraient pas pu être utilisés pour préserver l'ordre public, le juge souligne le caractère disproportionné de ces usages.

Au regard de ce qui précède, le juge a considéré la condition d'urgence comme remplie et a donc enjoint à la CC de Cœur Côte Fleurie d'effacer les données à caractère personnel recueillies et exploitées par le logiciel.

Cette décision rejoint la position de la Cnil concernant l'impossibilité de recourir à des caméras intelligentes, et notamment biométrique, sans l'adoption au préalable d'un cadre juridique adapté à sa mise en œuvre. Toutefois, cette décision a été rendue alors que la CC de Cœur Côte Fleurie ne s'était pas présentée à l'audience et n'avait donc pas pu assurer sa défense.

... dont les fonctionnalités biométriques ne sont pas mises en œuvre

À la suite de la décision rendue par le tribunal administratif de Caen, les juges des référés liberté des tribunaux administratifs de Lille[20]et de Nice[21] ont eu l'occasion de se prononcer respectivement concernant le recours au logiciel briefcam par les communes de Roubaix et de Nice. La CC de Cœur Côte Fleurie, n'ayant pu assurer sa défense en première instance, a quant à elle interjeté appel devant le Conseil d'État[22].

Dans le cadre de ces trois affaires, les controverses majeures portaient sur les fonctionnalités de reconnaissance faciale ou de toute autre analyse biométrique de ces dispositifs, jugées particulièrement attentatoires aux droits et libertés des individus. Cependant, les communes de Nice et de Roubaix ont démontré ne pas pouvoir recourir à de telles fonctionnalités sans qu'elles soient au préalable activées, action qu'elles n'avaient pas la capacité de réaliser d'elles-mêmes et qu'elles n'avaient jamais sollicitée. Il semblerait que les communes se limitaient donc à des utilisations spécifiques de ce logiciel et quelque peu diminuées par rapport à son objet initial.

Premièrement, la commune de Roubaix utilisait seulement le logiciel pour la recherche, *a posteriori*, de plaques d'immatriculation, sur réquisition judiciaire. Le juge a estimé que cet unique emploi ne constituait pas un traitement de données personnelles au sens des dispositions de la directive du 27 avril 2016, et donc qu'aucune atteinte à une liberté fondamentale n'était caractérisée. En conséquence, le tribunal administratif de Lille a rejeté la requête.

Quant à la ville de Nice, si elle a reconnu avoir expérimenté le logiciel briefcam lors d'événements spécifiques, elle a déclaré ne plus en faire usage au moment de la décision et ne jamais avoir activé la licence permettant de recourir aux fonctionnalités biométriques. Le juge administratif de Nice a donc considéré qu'il n'y avait pas lieu de se prononcer sur

l’urgence car aucune atteinte à une liberté fondamentale n’était caractérisée. La requête a par conséquent été rejetée.

Enfin, la CC de Cœur Côte Fleurie l’utilisait pour la recherche de plaques d'immatriculation *a posteriori* dans le cadre d'enquêtes et recourait au module « recherche » du logiciel, mais sans accéder aux images, et uniquement aux fins de réaliser des statistiques sur la mobilité. De surcroît, la mise en œuvre des injonctions du premier juge avait détérioré le logiciel, le rendant inexploitable pendant plusieurs semaines. Ainsi, le Conseil d’État a jugé, en tenant notamment compte de l’annonce de contrôle de la Cnil concernant l’usage de ce logiciel par les collectivités, que la condition particulière d'urgence, requise dans le cadre de l'article L. 521-2 du code de justice administrative, n’était pas remplie. Par conséquent, le 21 décembre 2023, le Conseil d’État a annulé l’ordonnance rendue en première instance par le tribunal administratif de Caen.

C'est donc en l'absence de preuve concernant l’utilisation des fonctionnalités biométriques de ces dispositifs que les recours ont été rejetés. Il est en revanche fort à parier que si ces fonctionnalités avaient été activées, en dehors de tout cadre légal, la solution retenue aurait été bien différente. On peut notamment constater que, même si la portée de cette décision reste limitée depuis l’intervention de l’ordonnance du juge des référés du Conseil d’Etat, le juge du tribunal administratif de Caen, qui n’avait pas connaissance du non-recours à ces fonctionnalités par la communauté de communes, avait jugé nécessaire la mise en œuvre de mesures de sauvegarde de nature à préserver le droit au respect de la vie privée.

---

[1] Cnil, position sur les conditions de déploiement, « Caméras dites « intelligentes » ou « augmentées » dans les espaces publics », juillet 2022.

[2] Conseil d’Etat, *Le numérique et les droits fondamentaux*, Étude annuelle, 9 septembre 2014, p. 16.

[3] Disclose, « *La police nationale utilise illégalement un logiciel israélien de reconnaissance faciale* », 14 novembre 2023.

[4] Cnil, position sur les conditions de déploiement, « Caméras dites ‘intelligentes’ ou ‘augmentées’ dans les espaces publics », juillet 2022.

[5] 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 (règlement général sur la protection des données).

[6] Directive 2016/680/UE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, du 27 avril 2016.

[7] Cnil, position sur les conditions de déploiement, « Caméras dites « intelligentes » ou « augmentées » dans les espaces publics », juillet 2022.

[8] Assemblée nationale, rapport d’information sur les enjeux de l’utilisation d’images de sécurité dans le domaine public une finalité de lutte contre l’insécurité, 12 avril 2023, p. 71.

[9] Loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, Art. 10.

[10] Céline Castets-Renard, Amélie Turci, « « Caméras augmentées » : un danger pour les libertés lors des Jeux Olympiques et Paralympiques (et au-delà) ? » », *Dalloz*. 1138,2023.

[11] 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 « JOP » n° 2023-380 du 19 mai 2023.

[12] Céline Castets-Renard, Amélie Turci, « « Caméras augmentées » : un danger pour les libertés lors des Jeux Olympiques et Paralympiques (et au-delà) ? » », *Dalloz*. 1138,2023.
[13] Conseil constitutionnel, décision n° 2023-850 DC, 17 mai 2023.
[14] Assemblée nationale, rapport d'information sur les enjeux de l'utilisation d'images de sécurité dans le domaine public une finalité de lutte contre l'insécurité, 12 avril 2023, p. 79.
[15] Proposition de Règlement 2021/0106/UE établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, 21 avril 2021, art 5.
[16] Contrôleur européen à la protection des données, Comité européen de la protection des données, « Avis conjoint 5/2021sur la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle », 18 juin 2021.
[17] Cnil, « Intelligence artificielle : l'avis de la CNIL et de ses homologues sur le futur règlement européen », 08 juillet 2021, consulté le 18/01/2024.
[18] Tribunal administratif de Caen, décision n° 2303004, 2303012, 22 novembre 2023.
[19] Directive 2016/680/UE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, du 27 avril 2016.
[20] Tribunal administratif de Lille, décision n°2310103, 2310163, 29 novembre 2023.
[21] Tribunal administratif de Nice, décision n°2305692, 2306593, 2305712, 23 novembre 2023.
[22] Conseil d'État, ordonnance n° 489990, 21 décembre 2023.

Références

- Loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions.
- Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure
- Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité
- 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 « JOP » n° 2023-380 du 19 mai 2023

SUR LE MEME SUJET

- Intelligence artificielle, innovation et collectivités locales
- Intelligence artificielle : les sénateurs veulent évaluer son potentiel... et ses dangers pour les collectivités
- L'intelligence artificielle, révolution contestée de la vidéosurveillance