La sécurité des Jeux : les libertés disqualifiées ?

Le cas de l'expérimentation des « caméras augmentées »

Maxime de la Bruyère

Doctorant à l'Université d'Aix-Marseille

De manière générale, le domaine de la sécurité suscite de vifs débats qui s'articulent autour de la traditionnelle tension entre liberté et sécurité. Aujourd'hui, la multiplication des procédés de surveillance numérique ravive les braises de ce débat. Ils sont présentés d'un côté comme le moyen désormais incontournable pour maintenir l'ordre, et de l'autre côté comme l'outil le plus intrusif jamais créé.

De manière plus spécifique à notre sujet, le sport vient souffler un vent très chaud sur ces braises. Les grands évènements sportifs, et toutes leurs implications matérielles, soulèvent d'importants enjeux en matière de sécurité. Il suffit pour s'en convaincre de se référer aux violences qui ont frappé la finale de la Ligue des Champions à Paris le 28 mai 2022[1].

C'est dès lors sans surprise que pendant tout le processus d'adoption de la loi du 19 mai 2023, la sécurité a occupé une place plus que prépondérante[2].

Dans cette loi, plusieurs dispositifs sécuritaires sont autorisés La présente étude se concentrera uniquement sur la plus controversée, à savoir l'utilisation de caméras de vidéoprotections équipées d'algorithmes. Il s'agit de l'article 10 qui au demeurant est le plus long de la loi (11 sections), et qui a préoccupé la plus grande partie des avis rendus par le CE et la CNIL, ainsi que la décision rendue par le Conseil constitutionnel.

Factuellement, cela correspond au déploiement d'un large parc de caméras fixes ou mobiles (drones) équipées d'un algorithme qui permet de traiter les images récoltées afin de signaler aux

[1] Voir par exemple le rapport sur l'organisation de la finale de Ligue des Champions de l'UEFA le samedi 28 mai 2022 au Stade de France et le renforcement du pilotage des grands évènements sportifs, publié par le Délégué Interministériel aux Grands Événements Sportifs et délégué interministériel aux Jeux Olympiques et Paralympiques le 10 juin 2022.

[2] 9 pages sur 18 de l'avis du CE sur le projet de loi y sont consacrées ; l'entièreté de la délibération à propos du projet de loi, à l'exception de l'article relatif aux données de santé pour la lutte contre le dopage, y est consacrée ; 13 pages sur 23 de la décision du Conseil constitutionnel sur cette loi y sont consacrées ; et un tiers des articles de la version de la loi entrée en vigueur y est consacré…

agents des évènements susceptibles de menacer la sécurité des personnes présentes (« caméras augmentées »).

Politiquement, c'est la première fois qu'un tel dispositif est légalement autorisé à une fin sécuritaire. Cette expérimentation divise les partisans d'une société plus sécuritaire et ceux inquiets par l'avènement d'une société de surveillance. C'est ce qu'illustre d'ailleurs la fronde levée par des associations de défense des libertés qui, pour l'occasion, ont ironiquement nommé la France « championne olympique de la technopolice »[3] ou encore « championne de la surveillance de masse »[4].

Mais qu'en est-il juridiquement ? Comment le droit encadre-t-il la mise en œuvre inédite des caméras augmentées à des fins sécuritaires ? C'est ce que le reste de cette étude va s'efforcer de présenter synthétiquement en étudiant le régime juridique (**I**) avant de mettre en avant ses faiblesses et d'en souligner sa potentielle portée (**II**).

I. Le régime juridique de l'utilisation des caméras augmentées

Pour étudier le régime juridique, il faut se référer prioritairement à l'article 10 de la loi du 19 mai 2023, enrichi de la lecture de la décision du Conseil constitutionnel du 17 mai 2023[5] ainsi que du décret d'application du 28 août 2023[6]. Il ne faut toutefois pas omettre le droit de l'Union européenne qui s'applique en raison de l'utilisation de données personnelles, notamment le RGPD et la directive Police-Justice transposée dans la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Il ressort de cette lecture globale un régime dense dont il convient ici d'aborder seulement les éléments les plus essentiels, propres à l'usage inédit de ces algorithmes. À ce titre, nous en retiendrons cinq.

Premièrement, s'agissant de la finalité et des conditions pour enclencher ce dispositif, le I de l'article 10 dispose qu'il est possible de les mettre en œuvre « à la seule fin d'assurer la sécurité de manifestations sportives, récréatives ou culturelles qui par l'ampleur de leur fréquentation ou par

[3] Article publié sur site de *La Quadrature du Net*, « Paris 2024 : La Franche championne olympique de la technopolice » disponible en ligne, consulté le 20 septembre 2023 ;

[4] Article publié sur le site internet du média indépendant *Reporterre*, « JO 2024 : la Franche championne de la surveillance de masse », disponible en ligne, consulté le 20 septembre 2023.

[5] Décision n° 2023-850 DC du 17 mai 2023 sur la loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions.

[6] 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.

leurs circonstances, sont particulièrement exposées à des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes ». Le Conseil constitutionnel estime que cette finalité et ces conditions sont suffisamment précises et circoncises, évitant alors un recours trop large et facile à ce mécanisme[7]. Il convient également de souligner, que le principe de finalité en droit des données personnelles s'applique aussi. Cela signifie que les données ainsi récoltées ne peuvent être utilisées qu'à cette fin, à l'exception éventuellement d'un usage statistique ou pour l'apprentissage de l'algorithme[8].

Deuxièmement, s'agissant du champ d'application, il s'apprécie spatialement et temporellement. À cette fin, le Conseil constitutionnel a ainsi vérifié que le déploiement du dispositif se cantonne bien aux lieux des manifestations et aux lignes de transports publics permettant d'y accéder ainsi qu'à la durée de l'évènement et guère plus[9].

Troisièmement, s'agissant de l'algorithme, dans la mesure où il sera certainement fourni par une entreprise privée, l'article 10 énonce plusieurs exigences à ce propos afin d'éviter les biais discriminatoires. Le Conseil constitutionnel vérifie aussi la présence d'un contrôle exercé par une personne humaine c'est-à-dire qu'il attend qu'une personne physique puisse, en se fondant sur des critères objectifs, vérifier que l'algorithme est efficace et non-discriminatoire, afin d'éventuellement le modifier au fur et à mesure[10].

Quatrièmement, s'agissant de l'objet du traitement, il ne se confond pas avec sa finalité puisqu'il correspond à ce que l'on va concrètement faire avec. Ici, le traitement sert uniquement pour « détecter, en temps réel, des événements prédéterminés susceptibles de présenter ou de révéler des risques et de les signaler en vue de la mise en œuvre des mesures nécessaires ». La liste de ces évènements a été précisée dans l'article 3 du décret du 28 août 2023, et on y trouve par exemple la « présence d'objets abandonnés » ; « l'utilisation d'armes » ; « le respect du sens de circulation » ou encore, de façon plus étonnante « une densité trop importante de personnes »[11]…

Toujours à propos de l'objet du traitement, il ressort également du contrôle opéré par le Conseil constitutionnel qu'il faut être attentif à au moins quatre éléments[12]. En premier lieu, l'objet doit

[7] Décision n° 2023-850 DC du 17 mai 2023, *op. cit.*, considérant 37.
[8] Article 5 b) du RGPD.
[9] Décision n° 2023-850 DC du 17 mai 2023, *op. cit.*, considérants 38 et 39.
[10] *Ibid.*, considérant 44.
[11] Voir *infra*, II.
[12] Décision n° 2023-850 DC du 17 mai 2023, *op. cit.*, considérants 41 à 44.

bien être en lien avec la finalité ce qui signifie concrètement que les évènements prédéterminés qui sont recherchés doivent être pertinents pour assurer la sécurité des personnes. En deuxième lieu, ces évènements ne doivent pas être susceptibles de créer des discriminations. En troisième lieu, l'objet du traitement doit être très circoncis ce qui empêche ici de croiser les données avec d'autres données récoltées, et évite ainsi le profilage. En dernier lieu, un critère déterminant est la primauté humaine dans le traitement des données : le traitement doit uniquement servir à signaler un éventuel problème à l'agent, qui aura ainsi le dernier mot en confirmant ou infirmant la situation. Dès lors, aucune décision ne doit être prise de manière automatisée.

Cinquièmement, s'agissant de la nature des données, c'est un élément fondamental pour apprécier la gravité de l'atteinte à la vie privée, et donc déterminant pour le contrôle réalisé par le Conseil constitutionnel. Il faut ici souligner que l'usage de données biométriques est prohibé par l'article 10, ce qui interdit ainsi la reconnaissance faciale.

Pour terminer, le reste du régime, notamment relatif à l'autorité compétente pour enclencher la procédure (autorité préfectorale et préfet de police de Paris), aux garanties qui entourent cette dernière, et aux personnes habilitées à accéder aux images, il n'est pas spécifique à ces caméras augmentées. Il est d'ailleurs possible d'y retrouver divers éléments qui font écho au droit européen des données à caractère personnel notamment le principe de finalité, de proportionnalité, de sécurisation et de conservation des données.

En résumé, on observe qu'il s'agit d'un régime juridique dont les détails témoignent de cette recherche de l'équilibre entre la préservation de la vie privée et la protection des personnes grâce à ces caméras augmentées. C'est d'ailleurs tout l'enjeu du contrôle opéré par le Conseil constitutionnel qui vérifie la présence de « garanties particulières de nature à sauvegarder le droit au respect de la vie privée »[13].

Cela dit, malgré ces efforts l'équilibre n'est pas tout à fait atteint (**II**).

[13] Décision n° 2023-850 DC du 17 mai 2023, *op. cit.*, considérant 33.

II. Les faiblesses du régime juridique : une protection des libertés faillible et une portée à ne pas sous-estimer

Comme il vient d'être dit, le régime juridique est composé de plusieurs garanties dont la finalité est de préserver le droit à la vie privée. Or, la cohérence entre la finalité de ces dispositions et leur contenu peut être discutée notamment pour trois d'entre elles.

En premier lieu, s'agissant des conditions pour limiter les situations pour lesquelles il est possible de mettre en œuvre ces dispositifs, l'effectivité de leur caractère limitant peut interroger. En l'espèce, dès lors qu'une manifestation atteint une certaine fréquentation, la sécurité physique des personnes y assistant peut, par définition, être menacée. En outre, « les circonstances » dans lesquelles un tel dispositif serait justifié ne sont pas précisées dans le décret d'application. Il en résulte donc, qu'il existe une marge d'appréciation certaine pour l'autorité publique pour savoir si elle peut ou non enclencher le dispositif. Il faudra ainsi être attentif aux occasions pendant lesquelles un tel mécanisme sera bien mis en œuvre pour voir si la pratique de la lettre correspond bien à l'esprit, à savoir de rendre exceptionnel l'usage de ces caméras.

En deuxième lieu, s'agissant de la nature des données, une controverse sur l'interprétation de la définition de donnée biométrique a été soulevée par des association de défense des libertés. Pour rappel, celle-ci est ainsi posée par le 14° de l'article 4 du RGPD :

> « les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux **caractéristiques physiques**, (…)ou **comportementales** d'une personne physique, qui permettent ou confirment son identification unique, telles que des **images faciales** (…) ».

Deux interprétations sont alors possibles. La première, soutenue par le législateur et le Conseil constitutionnel, consiste à dire qu'une donnée n'est biométrique que si elle est traitée de façon et dans le but d'identifier la personne par son comportement ou ses caractéristiques physiques comme son visage. La définition est alors composée d'un critère fonctionnel, il faut que l'objet du traitement soit d'identifier la personne. La seconde, celle soutenue par les associations de défense des libertés[14], consiste à dire que dès lors que la donnée récoltée est relative aux caractéristiques

[14] Voir à ce sujet, sur le site internet de La Quadrature du Net, plusieurs articles à ce sujet dont « Vidéosurveillance biométrique : derrière l'adoption du texte, la victoire d'un lobby », disponible en ligne, consulté le 20 septembre 2023 ;

physiques, en l'espèce l'image de nos visages, elle peut potentiellement permettre l'identification de la personne, ce qui suffit donc pour en faire une donnée biométrique. Cette ambiguïté n'est pas anodine car le régime juridique qui s'y appliquerait serait alors bien plus restrictif.

En dernier lieu, s'agissant de l'algorithme, il existe au moins deux angles morts. Le premier correspond au risque de discrimination et le second au contrôle éventuel par le public de ce risque c'est-à-dire la transparence de l'algorithme. Pour le premier, selon l'objet attribué à l'algorithme c'est-à-dire le type d'évènements recherchés, le traitement peut être discriminatoire en stigmatisant certaines personnes en raison de leur couleur ou de leur handicap. *A priori*, le décret d'application se préserve d'un tel écueil en énonçant des évènements qui semblent éviter ce genre de faiblesses. Il conviendra cependant, *a posteriori*, de vérifier que cela est bien le cas en pratique, en accédant éventuellement au code source de l'algorithme. En découle alors le second angle mort : le manque de transparence de l'algorithme. La transparence en matière d'algorithmes est en effet un moyen pour s'assurer de l'absence de discriminations. Or, celle-ci semble compromise pour au moins deux raisons. Dans un premier temps, à la lecture de la partie du Code des Relations entre le Public et l'Administration (CRPA) relative à la communication des documents administratifs[15], il semble qu'il n'est possible d'obtenir la communication du code source d'un algorithme uniquement lorsque celui-ci est au fondement d'une décision administrative individuelle, ce qui n'est pas le cas ici. Dans un second temps, même s'il était prouvé qu'il était possible de contourner cette condition, dans la mesure où ce code source est une propriété intellectuelle sur laquelle repose l'économie d'une entreprise, il est fort à parier que le secret des affaires ferait obstacle à cette communication, de façon tout à fait classique en matière de communication des documents administratifs. Au-delà, il pourrait même y avoir des risques en matière de cybersécurité à communiquer le code source, ce qui serait contreproductif. On voit donc qu'à propos de l'algorithme, l'élément central de ce dispositif, il existe bien des garanties sur son fonctionnement, mais qu'il existe tout de même encore des questionnements importants à propos de sa transparence.

Il résulte donc de tout cela que la capacité du régime à préserver les libertés est encore incertaine, tout comme d'ailleurs la portée réelle de cette expérimentation qui ne doit pas être sous-estimée.

CASTETS-RENARD C. et TURCI A., « Caméras augmentées » : un danger pour les libertés lors des Jeux Olympiques et Paralympiques (et au-delà) ? », *Recueil Dalloz*, 2023, p. 1138.

[15] Notamment les articles L300-2, L311-3-1, L312-1-3 : seule l'hypothèse d'une décision administrative individuelle semble être prise en compte.

Il est vrai qu'elle est très encadrée par une série de contrôle et de rapports, la fin de l'expérimentation étant d'ailleurs marquée par la remise d'un rapport à la CNIL. Dans son avis, elle précise même les éléments qu'elle souhaite voir apparaitre dans ce document afin d'évaluer l'expérimentation, et insiste à ce titre sur le fait qu'elle « ne saurait en aucun cas préjuger d'une éventuelle pérennisation de ces systèmes »[16]. Pourtant, plusieurs éléments peuvent faire penser que la portée de ce régime est plus large que celle attribuée à l'expérimentation, reléguant alors les JOP au rang de simple prétexte.

D'abord, la date de la fin de l'expérimentation a été contestée devant le Conseil constitutionnel puisqu'elle prend fin sept mois après la fin des JOP (31 mars 2025). L'argument pour justifier un tel délai était de dire qu'au vu de l'importance du choix de pérenniser ou non ce dispositif, il était nécessaire de se donner suffisamment de temps pour l'expérimenter. Si cela peut s'entendre, c'est déjà la preuve que les JOP n'étaient qu'un prétexte. Pour terminer de s'en convaincre, il suffit de revenir à la lettre de l'article 10 qui ne se limite pas aux évènements sportifs, ce que supposerait une loi dédiée aux JOP, mais s'étend également aux évènements « récréatifs ou culturels ».

Ensuite, et plus politiquement, on peut se demander si, au vu des sommes qui auront été engagées à la fin de l'expérimentation, les gouvernants oseront potentiellement admettre l'inefficience du dispositif. Quand on se réfère d'ailleurs à la liste des évènements prédéterminés, et qu'on y lit « densité trop importante de personnes » alors que par définition, plusieurs millions de personnes seront présentes en même temps, il est déjà possible de s'interroger sur l'efficacité des signalements[17]…

Enfin, et plus juridiquement cette fois-ci, la logique et les garanties qui composent ce régime font écho à celles qui composent déjà les régimes des autres dispositifs de surveillance, qui d'ailleurs ne sont pas exclusifs les uns des autres. Par exemple, à propos de l'exploitation des données de connexion récoltées auprès d'opérateurs privés à des fins de sécurité nationale, la CEDH[18], la CJUE[19] et le CE[20] adoptent le même raisonnement fondé sur la vérification de garanties particulières. Les mêmes éléments s'y retrouvent : des finalités laissant une marge d'appréciation

[16] Délibération 2022-118 du 8 décembre 2022, p. 5.
[17] Voir à ce sujet, MAUREL R., « Paris 2024 : « Réécrire le décret sur la vidéoprotection algorithmique est une nécessité pour éviter des dérives prévisibles », Tribune publiée dans le journal *Le Monde*, le 23 septembre 2023.
[18] CEDH, Gr. Ch., 25 mai 2021, n° 58170/13, 62322/14, 24960/15, *Big Brother Watch et autres c. Royaume-Uni.*
[19] CJUE, Gr. Ch., 6 octobre 2020, C 511/18, C 512/18 et C 520/18, *Quadrature du Net et autres* ; CJUE, Gr. Ch., 6 octobre 2020, C-623/17, *Privacy International.*
[20] CE, 12 février 2016, n°388134, *French Data Network et la Quadrature du Net.*

certaine à l'autorité publique, un champ d'application apprécié de la même façon, une gravité appréciée selon la nature des données, des garanties procédurales, les principes du droit européen des données, *etc*[21].

Tout cela prouve que la pérennisation du régime serait donc cohérente avec ce qui existe déjà dans le domaine, ajoutant une pierre supplémentaire à l'édifice du régime juridique de la surveillance. En outre, en cas de pérennisation du dispositif, les conditions actuellement posées et le contrôle relativement peu poussé du Conseil constitutionnel à leur égard semblent rendre juridiquement possible l'avancée d'une politique sécuritaire des petits pas vers des techniques de surveillance toujours plus efficaces et/ou intrusives (selon le point de vue adopté).

En conclusion, dans la relation entre JOP, sécurité, droit et libertés, le premier est un prétexte, le deuxième un projet, le troisième un moyen pour y parvenir, et le dernier un dommage collatéral.

[21] Voir plus précisément à ce sujet les actes du colloque « Les données de connexion - Quel équilibre entre droits fondamentaux et lutte contre la criminalité à l'ère du numérique ? », *RFDA,* 2023 p.603 et s., dans lesquels on y apprend l'activisme de la CJUE en matière d'exploitation des données de connexion par les États, son influence sur le raisonnement adopté par les juges nationaux notamment le Conseil d'État et le Conseil constitutionnel.