



HAL
open science

Le régime de surveillance olympique

Adrien Tallent

► **To cite this version:**

Adrien Tallent. Le régime de surveillance olympique. Revue Esprit, 2024, Juillet-Août (7), pp.16-19. 10.3917/espri.2407.0016 . hal-04727641

HAL Id: hal-04727641

<https://hal.science/hal-04727641v1>

Submitted on 9 Oct 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Le régime de surveillance olympique

Paru dans la *Revue Esprit*, numéro juillet/août 2024, pp. 16-19

TALLENT, Adrien. « Le régime de surveillance olympique ». *Esprit*, 2024/7 Juillet-Août, 2024. p.16-19.

*Adrien Tallent*¹

¹ Sciences, Normes, Démocratie (SND), Sorbonne Université, CNRS, Paris, France

Les jeux olympiques et paralympiques qui se dérouleront à Paris cet été nous font-ils entrer dans une société de surveillance ? C'est du moins un risque mis en avant par certains acteurs et associations. La vidéosurveillance algorithmique (VSA) a en effet été autorisée pour la première fois en France à titre expérimental dans le cadre de la loi relative aux Jeux Olympiques et Paralympiques de 2024 « *dans un cadre légal clair et préservation des libertés fondamentales et individuelles* »¹. Cette loi autorise l'utilisation de la VSA jusqu'au 30 juin 2025, date à partir de laquelle elle devrait être rediscutée.

Répondre à un enjeu sécuritaire ?

L'expérimentation de la VSA est justifiée par l'exécutif par les enjeux sécuritaires que pose l'organisation des Jeux Olympiques et paralympiques à Paris, notamment la cérémonie d'ouverture (600 000 personnes attendues initialement). Un décret adopté le 28 août 2023 a précisé les événements que ces logiciels devront détecter : présence d'objets abandonnés, utilisation d'armes, mouvements de foule, départs de feu, chutes, non-respect du sens de circulation, intrusion dans des zones interdites ou sensibles, densité excessive de personnes. Le but est d'éviter les mouvements de foule mortelle mais aussi, et surtout, d'anticiper les risques d'attentats terroristes. Des solutions algorithmiques vont alors analyser les images issues des caméras ou de drones pour détecter et signaler en temps réel des comportements anormaux ou suspects.

Si le gouvernement se défend de toute surveillance « biométrique » puisque le texte n'autorise pas explicitement la reconnaissance faciale en temps réel – par ailleurs interdite par la réglementation européenne –, les travaux de l'association La Quadrature du Net démontrent pourtant qu'il s'agit d'un mensonge. « *Cette technologie identifie, analyse, classe en permanence les corps, les attributs physiques, les gestes, les silhouettes, les démarches, qui sont incontestablement des données biométriques* »².

L'installation de pareils dispositifs de surveillance provient d'une forme de double autojustification. D'abord, l'exigence sécuritaires imposerait un nombre toujours plus grand de caméras, jusqu'à devenir trop nombreuses pour l'œil humain. Alors, pour gérer la masse, la VSA serait la seule solution. Ensuite, les Jeux Olympiques semblent être la justification idéale pour adopter la VSA, déjà légalisée ou expérimentée dans

¹ « Lancement de l'expérimentation « vidéo-intelligentes » en vue de la sécurisation des Jeux Olympiques », *site du Ministère de l'Intérieur*

² La Quadrature du net, « La France premier pays d'Europe à légaliser la surveillance biométrique », 23 mars 2023

un certain nombre de villes et de pays. L'élargissement de l'expérimentation à tous les événements publics importants (compétitions sportives, festivals...) tend à justifier cette affirmation. De la même manière, des caméras associées à des solutions d'intelligence artificielle seront déployées dans le métro mais ne seraient utilisables qu'a posteriori dans le cadre d'enquêtes judiciaires et sous contrôle d'un juge.

Un panoptique idéalisé

Les arguments sécuritaires avancés sont toujours identiques. Il s'agit de repérer les comportements, ou les émotions, qui sortent de la norme. Cette notion de norme est dès lors sujette à interrogation. Dans le cas des festivals de musique par exemple, certains comportements dits « anormaux » sont la norme dans ce contexte particulier. Toute la justification du gouvernement revient à dire que ces algorithmes ne feront que pointer les comportements anormaux aux agents en charge de visionner les vidéos. Ce ne serait donc qu'un outil d'assistance pour des agents physiquement incapables de gérer le flot d'images.

La promesse est donc double : un outil technologique neutre associé à une intervention humaine en bout de chaîne. La première a depuis longtemps été contredite. Socrate accuse Gorgias de manipulateur tandis que pour Heidegger, la technique moderne n'est pas un moyen neutre, mais un mode de « dévoilement » qui enferme l'être dans une vision utilitariste et productiviste. Pourtant cette opinion est tenace parmi les promoteurs d'une idéologie de la surveillance à grande échelle. Les algorithmes utilisés dans ce type de surveillance automatisée sont entraînés sur des données reflétant les biais raciaux, ethniques et genres de nos sociétés. Ces bases de données servent à définir une « normale » qui n'a donc rien d'objectif. Cette pensée témoigne également d'une confiance excessive dans les machines et l'automatisation des tâches en général. Si le gouvernement promet une décision humaine en fin de chaîne, quid de la protection (et donc de l'intérêt) de l'agent humain qui ira contre les recommandations de la machine ?

Discrets, presque invisibles, les dispositifs de surveillance (capteurs, caméras) voient sans être vus. Ils dévoilent le réel. Leurs fonctions s'exercent en silence tandis que les données qu'ils transmettent sont imperceptibles. En ce sens, ils semblent participer d'une forme de panoptique benthamien.

La sécurité est la première des libertés

Le recours à la surveillance automatisée s'inscrit également dans un discours politique, affirmant que la sécurité serait la première des libertés. Pour ses adeptes, l'intelligence artificielle (IA) résout le problème majeur de la surveillance vidéo, à savoir la difficulté d'analyser de très grandes quantités d'images. Dès lors, le discours sécuritaire visant à installer toujours plus de caméras a pour conséquence logique la promotion de ces solutions. Pourtant, le recours à de tels outils provient du mythe de leur infailibilité. Déjà dans les années 1920, des premiers modèles statistiques et sociologiques avaient pour objectif de prédire les crimes et les délits. Aujourd'hui, de nombreuses entreprises s'engouffrent dans cette brèche en promettant aux autorités des logiciels de prédiction des crimes, de traçage ou de VSA. Néanmoins, il convient de rappeler que ces solutions sont imparfaites, biaisées et sources de discriminations, et qu'aucune surveillance n'empêche les délits d'être commis, mais déplace leurs lieux de réalisation. Ce solutionnisme technologique ne répond qu'à l'angoisse sécuritaire alimentée par des discours politiques.

Cette expérimentation olympique s'inscrit alors dans une généalogie de la *technopolice*. En France, en 2019, la ville de Nice a par exemple voulu tester la reconnaissance des émotions dans la ville. En 2018, c'est la région Provence-Alpes-Côte-D'Azur qui a voulu installer un logiciel de reconnaissance faciale dans les lycées. Mais c'est avec la pandémie due au Covid-19 que de nombreux systèmes de surveillance et de traçage ont été déployés dans l'espace public et ont forgé l'accoutumance du grand public à ses technologies invasives destinés à être temporaires mais qui se sont généralisées (drones policiers, QR code pour accéder à certains lieux pendant les JO...).

Cette expérimentation olympique s'inscrit dans une généalogie de la *technopolice*. En France, en 2019, la ville de Nice a par exemple voulu tester la reconnaissance des émotions dans la ville. En 2018, c'est la région Provence-Alpes-Côte d'Azur qui a voulu installer un logiciel de reconnaissance faciale dans les lycées. Mais c'est avec la pandémie due au Covid-19 que de nombreux systèmes de surveillance et de traçage ont été déployés dans l'espace public et ont forgé l'accoutumance du grand public à ces technologies envahissantes destinées à être temporaires mais qui se sont généralisées (drones policiers, QR code pour accéder à certains lieux pendant les JO...).

Un système qui n'a jamais fait ses preuves

La vidéosurveillance « intelligente » suscite de vives critiques quant à son efficacité. Malgré l'absence de preuves solides de son efficacité, les entreprises espèrent démontrer le contraire. En 2022, la Commission nationale de l'informatique et des libertés (CNIL) a souligné que la VSA représente bien plus qu'une simple amélioration des dispositifs existants. En abolissant les limites humaines, ces technologies permettent une surveillance plus exhaustive et invisible des lieux publics où s'exercent certaines libertés fondamentales. Dès lors, elles opèrent un « changement de nature » dans la surveillance de l'espace public³. Mais des exemples passés montrent également les limites de ces technologies. En 2016, la SNCF a testé des caméras « intelligentes » pour détecter les agressions, sans en communiquer les résultats. En 2017, à Londres, une expérience de reconnaissance faciale au carnaval de Notting Hill a échoué avec de nombreux « faux positifs ».

Cette adoption de la VSA est officiellement temporaire. Toutefois, il est peu probable qu'elle ne soit pas pérennisée. De ce point de vue, les JO semblent servir de cheval de Troie pour cette technologie. La VSA s'inscrit dans un contexte plus large d'une automatisation de la surveillance et des politiques de promotion de la *Smart City* dans laquelle s'instituerait une gouvernance par les données (de plus en plus de processus décisionnels sont ainsi délégués à des solutions fondées sur de l'IA). Cet « *état d'urgence technologique* »⁴ s'impose à bas bruit, profite d'événements exceptionnels (terrorisme, JO, pandémie...) et tend à normaliser des mesures ponctuelles, complexifiant tout retour à la normale. La question reste ouverte de savoir jusqu'où nous irons dans l'adoption de ces technologies de surveillance.

³ CNIL, « caméras dites « intelligentes » ou « augmentées » dans les espaces publics », Juillet 2022

⁴ Voir Olivier Tesquet, *Etat d'urgence technologique*, Premier Parallèle, 2021