Médaille d'or de la surveillance, pour la France ?

Pour sécuriser les Jeux olympiques de l'été 2024 une loi spécifique a été votée, qui prévoit le déploiement à grande échelle de techniques de surveillance faisant appel à l'intelligence artificielle. Une « expérimentation » à hauts risques pour nos données personnelles.

Maryse ARTIGUELONG, membre du bureau national de la LDH

Pour ce grand évènement sportif que sont les Jeux olympiques (JO), plusieurs villes de France (Paris, Bordeaux, Marseille, Lille…) accueilleront, selon la DGSI[1], du 26 juillet au 8 septembre 2024, 15 000 athlètes, 12 millions de spectateurs, 45 000 volontaires, 25 000 journalistes et environ 100 chefs d'Etat. Dans un contexte de menaces multiples (terrorisme, cyberattaques…), la sécurité constitue un enjeu particulièrement important. Le gouvernement a donc fait voter le 12 avril 2023, en procédure accélérée[2] – alors que les JO ont été attribués à Paris en 2017 –, la loi relative aux Jeux olympiques et paralympiques de 2024 (JOP 2024). Entrée en vigueur dès le 19 mai 2023, elle introduit l'expérimentation d'outils numériques (vidéosurveillance algorithmique ou « VSA », scanners corporels, criblage) qui menacent les droits et libertés.

L'expérimentation de la VSA

Selon le ministère de l'Intérieur, la vidéosurveillance nécessaire pour assurer la sécurité des JOP exige la captation d'une quantité d'images telle que leur visionnage par des humains devient inopérante pour déceler des menaces. Le gouvernement a donc choisi le « technosolutionnisme » qui utilise l'intelligence artificielle (IA) pour les analyser et générer des alertes en cas de détection d'« événements prédéterminés » potentiellement générateurs de « risques ». L'article 10 de la loi[3] autorise ainsi l'expérimentation de la VSA : les images captées par les caméras de surveillance installées sur les sites olympiques et leurs « abords », dans les lieux accueillant des manifestations sportives, récréatives ou culturelles, dans les transports publics et leurs « emprises », ou encore sur des aéronefs (drones), seront analysées par des algorithmes conçus pour détecter des « comportements suspects » qui pourraient révéler des risques pour la sécurité.

> « Il faut savoir que tous les salariés ou bénévoles travaillant sur les sites des JO (soit environ soixante-mille personnes) devront obligatoirement faire l'objet d'une enquête administrative préalable avec consultation de plusieurs fichiers de police. Soit un criblage massif… »

La définition de ces « évènements » a été renvoyée à un décret[4] publié ensuite le 30 août 2023, empêchant de ce fait les législateurs d'examiner toute la portée de cette surveillance et la constitutionnalité de mesures restreignant les droits et libertés, mesures qui devraient, selon la loi Informatique et libertés[5], être appropriées, nécessaires et proportionnées. Ce décret a bien été soumis à l'avis de la Cnil[6], mais celle-ci n'a pas de pouvoir contraignant pour s'opposer aux atteintes à la protection de la vie privée.

Le texte autorise à titre expérimental, et jusqu'au 31 mars 2025 (donc bien au-delà de la fin des JOP !), le recours à des traitements algorithmiques sur les images collectées. Le décret liste les « évènements prédéterminés […] susceptibles de présenter ou de révéler un risque d'acte de terrorisme ou d'atteinte grave à la sécurité des personnes : présence d'objets abandonnés, présence ou utilisation d'armes, non-respect par une personne ou un véhicule du sens de circulation commun, franchissement ou présence d'une personne ou d'un véhicule dans une zone interdite ou sensible, présence d'une personne au sol à la suite d'une chute, mouvement de foule, densité trop importante de personnes, départs de feux ». La détection de ces évènements déclenchera une alerte pour la « […] mise en œuvre des mesures nécessaires par les services de la police nationale et de la gendarmerie nationale, les services d'incendie et de secours, les services de police municipale et les ser-

(1) Direction générale de la sécurité intérieure.

(2) Il n'y a donc eu qu'un seul examen dans chaque assemblée, le texte final ayant été validé par une commission mixte paritaire. Cette méthode, dénoncée à plusieurs reprises par la CNCDH, ne permet pas les nécessaires échanges sur des sujets techniques complexes entre parlementaires, et entre ces derniers et des experts et des citoyens.

(3) Voir www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000047561989.

(4) Voir www.legifrance.gouv.fr/jorf/id/JORFTEXT000048007135.

(5) Qui a intégré le règlement général sur la protection des données (RGPD) et la directive Police-Justice.

(6) Commission nationale de l'informatique et des libertés.

vices internes de sécurité de la SNCF et de la Régie autonome des transports parisiens dans le cadre de leurs missions respectives ». Or la sûreté nationale doit être assurée par les seules forces de police et de gendarmerie. Déléguer à d'autres services comme la SNCF ou la RATP pose la question de la délégation d'une prérogative régalienne à la sécurité privée. Par ailleurs, selon la Cour des comptes, le recrutement d'agents de sécurité semble difficile, le renfort de l'armée est même envisagé, ainsi que le recrutement d'étudiants étrangers ! Seront-ils formés à la protection des données personnelles ? Et la Cnil déplore le trop grand nombre de personnes qui auront accès aux images.

Algorithmes, biométrie et transparence

Le décret rappelle que ces traitements « n'utilisent aucun système d'identification biométrique, ne traitent aucune donnée biométrique [...] ». C'est pourtant ce qui avait motivé l'interpellation [7] de nos élus par trente ONG européennes et mobilisé nos organisations (OLN) [8] pour soutenir un mémoire en appui du recours au Conseil constitutionnel de parlementaires, démontrant la nécessaire utilisation de la biométrie pour détecter des événements impliquant des personnes dans les images capturées. Il est en effet nécessaire d'analyser les caractéristiques physiologiques et les comportements des individus présents à l'image (position du corps, démarche, gestes ou apparence), de les isoler de l'arrière-plan, sans quoi il serait impossible d'atteindre l'objectif poursuivi. Cette analyse équivaut, selon le RGPD [9], à l'utilisation de données biométriques. Or prédire les comportements, classer les personnes comme ayant un comportement « à risque », sur la base de ces données, fait peser des risques graves sur les droits fondamentaux. Le déploiement de la VSA dans l'espace public où la préservation de l'anonymat est essentielle constitue une menace pour les libertés (d'aller et venir, d'expression, de réunion, de manifestation…), d'autant plus que les traitements algorithmiques sont sujets à des résultats discriminatoires en raison de biais dus soit à la conception (choix des critères, orientation…), soit à la représentativité des différentes « populations » dans les bases de données qui les alimentent (biais statistiques).

Le décret rappelle que les traitements « n'utilisent aucun système d'identification biométrique, ne traitent aucune donnée biométrique [...] *». Or il est nécessaire d'analyser les caractéristiques physiologiques et les comportements des individus présents à l'image, de les isoler de l'arrière-plan, sans quoi il serait impossible d'atteindre l'objectif poursuivi. Cette analyse équivaut, selon le RGPD, à l'utilisation de données biométriques.*

Ces solutions algorithmiques seront développées par des entreprises privées puis intégrées aux systèmes de vidéosurveillance existants dans les zones où les préfectures en feront la demande (les arrêtés devraient permettre de connaître les emplacements, la nature et la durée de la surveillance). Ces entreprises devraient être auditées et certifiées, mais il est à craindre qu'elles ne se retranchent derrière le secret des affaires, pour y échapper. Pour être conforme au RGPD, la loi prévoit que les personnes seront informées par tout moyen approprié, ce qui laisse dubitatif sur la réalité de cette information concernant notamment les images captées par des drones, dont certains préfets font un usage immodéré [10]. La Cnil recommande qu'une information soit donnée sur le lieu de l'opération au cours de laquelle les caméras aéroportées seront utilisées, par exemple via des dispositifs sonores dont on demande à « entendre » l'efficacité…

Un dispositif contestable à tous égards

Le périmètre de l'expérimentation pose question. La loi comme le décret s'appliquent à tout le territoire y compris l'outre-mer où, hormis Tahiti, aucune épreuve n'est prévue, ce qui laisse à penser que l'expérimentation sera étendue au-delà des JOP. Quant au périmètre des caméras concernées, il semble bien difficile de délimiter juridiquement ou administrativement les « abords » des sites ainsi que les « emprises » SNCF ou RATP.

La loi prévoit en outre l'extension de l'usage des scanners corporels (« dispositifs d'imagerie utilisant des ondes millimétriques »), qui seront multipliés pour faciliter l'accès aux manifestations sportives, récréatives ou culturelles rassemblant plus de trois-cents spectateurs (donc pas limités aux JOP). Cette technologie, permettant de détecter des armes, produit une image virtuelle en 3D du corps nu qui peut révéler des données de santé (prothèses, implants, transidentité…). Ce sont des données sensibles qui ne devraient pas être collectées sans l'information et le consentement explicite de la personne concernée. Bien que soit prévue la possibilité de choisir un autre dispositif de contrôle (palpations réalisées par un agent de sécurité), cette option plus lente (deux-cents personnes par heure contre huit-cents) n'aura sans doute pas la faveur des spectateurs, augmentant faussement l'acceptabilité d'une technologie particulièrement intrusive dans l'intimité des personnes.

Il faut par ailleurs savoir que tous les salariés ou bénévoles travaillant sur les sites des JO (soit environ soixante-mille per-

« Il est à craindre que l'acceptabilité de la surveillance soit forte car les spectateurs seront plus focalisés sur leurs accès aux compétitions, aux spectacles, plutôt que sur la protection de leurs données personnelles et le respect de leur vie privée. Il sera donc facile de la pérenniser. »

© LICENCE PIXABAY

« Bien qu'annoncé pour la période des Jeux, le texte s'applique de mai 2023 à fin mars 2025. On peut redouter, compte tenu de la confiance des pouvoirs publics dans ces technologies et des investissements coûteux, que celles-ci ne soient pas abandonnées à la fin de cette période. »

sonnes, selon l'exposé des motifs) devront obligatoirement faire l'objet d'une enquête administrative préalable avec consultation de plusieurs fichiers de police. Soit un criblage massif… Selon la Cnil seraient consultés notamment le traitement des antécédents judiciaires (TAJ), critiqué à de nombreuses reprises [11], le fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT), au sujet duquel la CNCDH a émis de vives critiques [12], en raison de l'atteinte aux droits fondamentaux.

Enfin, quid de l'acceptabilité de ce type de surveillance ? L'introduction de la VSA à l'occasion des JO est un moyen de l'évaluer, et il est à craindre qu'elle soit forte dans la mesure où les spectateurs seront plus focalisés sur leurs accès aux compétitions, aux spectacles et autres fêtes plutôt que sur la protection de leurs données personnelles et le respect de leur vie privée. Il sera donc facile de conclure que cette technologie est acceptable, et de la pérenniser. Ce d'autant plus qu'une grande partie de la population est déjà favorable à la vidéosurveillance avec la « croyance », non vérifiée scientifiquement, en son efficacité. Ceci est d'autant plus dangereux que les responsables de la sécurité, trop confiants dans la VSA, pourraient relâcher leur vigilance et laisser survenir des actes que cette technologie prétend empêcher.

Mesures liberticides : l'« effet cliquet »

Bien qu'annoncé pour la période des Jeux, le texte s'applique de mai 2023 à fin mars 2025. On peut redouter, compte tenu de la confiance des pouvoirs publics dans ces technologies et des investissements coûteux, que celles-ci ne soient pas abandonnées à la fin de cette période. Comme dans le passé, d'autres lois sécuritaires annoncées comme temporaires ont été prolongées puis pérennisées (ainsi les dispositions dérogatoires de l'état d'urgence ont été intégrées dans la loi en 2017). D'ores et déjà, des parlementaires ont déposé deux propositions de loi (PPL) :

- l'une autorisant l'utilisation par la police et la gendarmerie de logiciels de reconnaissance biométrique dans l'espace public, pour faciliter la collecte de preuves d'infractions et l'identification de leurs auteurs, ou la recherche d'une personne disparue ou en fuite ;
- l'autre, « relative au renforcement de la sûreté (sic !) [13] dans les transports », autoriserait les services internes de sécurité de la RATP et de la SNCF à fournir des images pour répondre à des réquisitions judiciaires, et à collecter et traiter des données sensibles, dans le cadre du traitement d'infractions flagrantes punies d'une peine de prison.

Ainsi, sans même attendre le bilan des expérimentations de la loi JOP, ces élues et élus tentent d'élargir l'utilisation de techniques de surveillance particulièrement intrusives. La loi JOP 2024 comme ces PPL ne respectent pas les principes de nécessité et de proportionnalité qu'exige le respect des droits de l'Homme dans une démocratie, et ne font que confirmer la tendance à une surveillance généralisée liberticide.

Nous ne pouvons que soutenir les conclusions du rapport de mars 2023 [14] de la rapporteuse spéciale de l'ONU sur la promotion et la protection des droits de l'Homme dans la lutte antiterroriste, Fionnuala Ní Aoláin, mettant en garde contre « […] *l'augmentation alarmante de l'utilisation de technologies intrusives et à haut risque – notamment les drones, la biométrie, l'intelligence artificielle (IA) et les logiciels espions – dans la lutte mondiale contre le terrorisme, sans tenir compte de l'Etat de droit, de la gouvernance et des droits de l'Homme* ». ●

(7) Voir www.lemonde.fr/idees/article/2023/03/06/les-mesures-de-videosurveillance-algorithmique-introduites-par-la-loi-jo-2024-sont-contraires-au-droit-international_6164276_3232.html.

(8) Observatoire des libertés et du numérique.

(9) Règlement général sur la protection des données.

(10) Voir les nombreux recours de la LDH contre ces utilisations, notamment ceux mentionnés ici : www.ldh-france.org/utilisation-de-drones-dans-le-cadre-de-la-mobilisation-agricole/ ; www.ldh-france.org/les-drones-ou-la-nouvelle-recrue-des-forces-de-lordre/.

(11) La LDH, la Quadrature du Net, la Cnil, la Cour européenne des droits de l'Homme ont régulièrement critiqué le TAJ (dans lequel toute personne ayant été suspecte est fichée) pour atteinte disproportionnée au respect de la vie privée. En 2021 il contenait déjà 18,9 millions d'habitants et plus de 8 millions de photos non anthropométriques (réseaux sociaux, vidéosurveillance…). En 2022 le Conseil d'Etat a autorisé la reconnaissance faciale à l'aide des données du TAJ (375 747 demandes avaient déjà été faites par les services de police en 2019).

(12) Voir l'avis de la Commission nationale consultative des droits de l'homme : www.legifrance.gouv.fr/jorf/id/JORFTEXT000036758063. Ces mesures mettent en cause le respect des droits et libertés fondamentaux alors même qu'elles ne reposent pas sur une conception solide et éprouvée du concept de « radicalisation », mais essentiellement sur un objectif de *prédiction des comportements*, dans le but d'éviter tout acte terroriste.

(13) La confusion est fréquente entre « sécurité » et « sûreté »… C'est le mot « sécurité » qui aurait dû être employé ici, la « sûreté » étant « […] un droit qui protège les individus contre les arrestations et les emprisonnements arbitraires » (garanti d'ailleurs par l'article 2 de la DDHC de 1789).

(14) Voir www.ohchr.org/en/press-releases/2023/03/alarming-misuse-high-risk-technologies-global-fight-against-terrorism-says.