Sécuriser les JOP 2024 : quelle place pour la technologie ?

Par Julie MERCIER
Directrice des entreprises et partenariats de sécurité et des armes – ministère de l'Intérieur et des Outre-mer

Par leur ampleur – près de 15 millions de spectateurs attendus – et leur philosophie – des Jeux au cœur de la Ville –, les Jeux Olympiques et Paralympiques de Paris 2024 (JOP) revêtent un enjeu de sécurité inédit, accentué par un niveau de menace très élevé.

Alors que la mobilisation des forces de sécurité intérieure et, plus largement, de l'ensemble des acteurs du continuum de sécurité (polices municipales, acteurs de la sécurité privés, etc.) sera sans précédent, cet article précise comment la technologie contribuera, elle aussi, à relever ce défi, grâce notamment aux opportunités offertes par la loi du 19 mai 2023, sans nier, pour autant, les enjeux juridiques et sociétaux persistants.

Les défis de la sécurisation des JOP

Un défi sécuritaire propre à la physionomie unique des Jeux

La sécurisation des prochains Jeux Olympiques et Paralympiques de Paris 2024 (JOP) représente un défi d'une ampleur inédite.

Alors qu'ils s'insèrent dans un calendrier national déjà riche en événements majeurs (80e anniversaire du débarquement, Euro de foot, Tour de France, fête nationale), les JOP représentent en magnitude environ 40 fois l'organisation d'une Coupe du monde de football et plus de 100 fois celle d'une Coupe du monde de rugby comme celle récemment organisée en France.

Cette ampleur sans précédent ne se caractérise pas seulement par les 15 millions de spectateurs attendus, la multiplicité des événements simultanés ou leur enchaînement soutenu, mais également par l'élongation géographique. Ce sont ainsi 12 départements qui accueilleront une ou plusieurs épreuves olympiques, y compris en Outre-mer. À cette élongation géographique s'ajoute une élongation temporelle inhabituelle, de l'arrivée de la flamme à Marseille le 8 mai à la cérémonie de clôture le 8 septembre, qui distingue les JOP d'autres grands événements, comme, par exemple, un sommet de chefs d'État.

Mais au-delà de l'ampleur, c'est la philosophie même de Jeux au cœur de la Ville qui rend le défi sécuritaire unique : épreuve de tir à l'arc sur l'esplanade des Invalides, escrime au Grand Palais, *skate-board* à la Concorde, *beach-volley* à la Tour Eiffel, triathlon sur le pont d'Iéna, etc. La cérémonie d'ouverture marquera le point d'orgue avec les 90 bateaux des 206 équipes olympiques traversant la Seine, la présence de 150 à 200 chefs d'État et près de 600 000 spectateurs.

Dans un contexte de tensions internationales et de menaces sans précédent

Aux enjeux de sécurité spécifiques liés à la physionomie même des Jeux, s'ajoute un état de la menace particulièrement élevé. Aux côtés de la menace terroriste et contestataire persistante, le contexte international s'est significativement dégradé, avec le retour des stratégies de compétition entre les États-puissances, des affrontements régionaux décomplexés et la guerre aux portes de l'Europe. L'environnement stratégique s'est par ailleurs complexifié, avec la multiplication des modes d'action hybrides (drones, cyberattaques, etc.). Cet état de la menace n'est pas propre aux JOP mais, avec une audience attendue d'1,5 milliard de téléspectateurs, ils en seront le catalyseur.

Quelle place pour les technologies dans ce dispositif ?

Dès lors, face à cette équation sécuritaire inédite, quelle place la technologie peut-elle prendre aux côtés des 35 000 membres des forces de sécurité intérieure et 18 000 acteurs de la sécurité privée déployés en moyenne chaque jour, sans parler des polices municipales (dont 2 000 hommes/jour juste pour Paris) ?

Le Janus technologique : contrer les menaces que la technologie crée

Depuis 25 ans, le numérique a pris une place considérable dans l'organisation et la médiatisation des Jeux Olympiques. Cette transformation profonde est également source de menaces accrues. Les organisateurs de Paris 2024 s'attendent ainsi à huit à dix fois plus de cyberattaques par rapport aux 450 millions d'attaques détectées à l'occasion des Jeux de Tokyo. Un dispositif de sécurité « cyber » sans précédent est aujourd'hui déployé. Outre l'intégration de la sécurité « par conception », un centre de supervision « cyber », classique dans le public ou l'entreprise, mais encore assez rare dans l'événementiel sportif, a été mis en place. Des tests d'intrusion recourant aux technologies les plus avancées sont réalisés en continu et des exercices d'ampleur sont régulièrement organisés.

Autre défi technologique : la lutte anti-drone, réalisée pour les JOP 2024 à une échelle inédite, en particulier en Île-de-France. Couplant des systèmes lourds et plusieurs dizaines d'équipes légères déployées simultanément, sur la base d'une coordination interministérielle éprouvée à l'occasion de plusieurs exercices, le dispositif combinera plusieurs technologies : systèmes de brouillage, lasers anti-drone, drone d'interception, etc.

Le recours à la technologie : une garantie d'efficience et de discrétion

Mais au-delà d'un recours à la technologie pour contrer les menaces qu'elle génère, le vrai défi est de pouvoir se doter des réponses nécessaires à une plus grande efficacité, au travers d'un mix homme-machine le plus performant possible.

Pour atteindre cet objectif, l'enjeu a consisté à rechercher des technologies à même de compléter utilement la tâche des forces de sécurité ou des acteurs de la sécurité privée. Outre les dispositifs classiques (portiques de détection notamment), de nombreuses solutions ont été développées pour délester les intervenants des opérations les plus fastidieuses ou liées au contexte international particulier des Jeux : logiciels de "*speech to translate"* pour faciliter la prise en charge des plaintes des spectateurs étrangers, tablettes didactiques reprenant les procédures opérationnelles de base, etc.

La nouvelle technologie la plus emblématique est bien sûr celle de la vidéo-augmentée, qui, pour la première fois depuis la position de la Cnil de juillet 2022[1], sera testée dans un cadre légal clarifié.

L'objectif de cette expérimentation qui prohibe la reconnaissance faciale et toute forme de recoupement avec des fichiers est de déterminer sans *a priori* les apports possibles de solutions algorithmiques, éthiques et de confiance, à la sécurisation des grands événements, en facilitant le travail des opérateurs de vidéoprotection sans jamais se substituer à eux.

Rigoureusement sélectionnées dans le cadre d'un marché national conduit d'août à décembre 2023, les solutions déployées permettront de détecter automatiquement huit types d'événements : non-respect du sens de circulation, franchissement ou présence dans une zone sensible ou interdite, mouvement de foule, densité trop importante de personnes, colis abandonnés, présence ou utilisation d'armes, personne au sol, départs de feux.

Des premiers tests de paramétrages ont été réalisés en mars, suivis depuis de plusieurs déploiements opérationnels. À terme, ce seront plusieurs centaines de flux vidéo qui seront activés en simultané pendant la période des Jeux.

En complément de la recherche d'efficience, le recours à certaines solutions technologiques (vidéoprotection, hyperviseurs, drones de surveillance) doit également permettre de rendre le dispositif sécuritaire moins visible. En effet, pour que les Jeux restent une fête, le dispositif de sécurité doit non seulement être performant, mais surtout être le moins visible possible.

Le choix de technologies principalement matures sans pour autant exclure les expérimentations

Au vu des enjeux d'efficacité, contrairement à une idée reçue, l'objectif principal des organisateurs et des forces de sécurité n'est pas de recourir à des technologies innovantes, mais bien à des technologies matures, aux concepts d'emploi éprouvés et sur lesquels les opérateurs ont pu être formés dans la durée et ce d'autant que la nécessaire interopérabilité des différentes couches d'acteurs impose de travailler très largement en amont sur la coordination des moyens et des procédures.

Pour autant, la préparation des JOP 2024 a été l'occasion, pour le ministère de l'Intérieur et des Outre-mer, en lien avec la filière des industries de sécurité, de conduire un vaste programme d'expérimentation.

200 expérimentations ont ainsi été conduites sur 18 mois de 2021 à début 2023, à partir des conclusions d'ateliers d'expression des besoins qui ont réuni des services opérationnels aux modes d'action différents (police, préfecture de police, gendarmerie, sécurité civile, services d'incendie et de secours, services de renseignements, etc.) et même, dans certains cas, des services de sécurité privée (RATP, SNCF, aéroports de Paris, etc.). Les ateliers ont porté sur des scénarios de crises et de menaces comme le relais de la flamme, les *fanzones*, les axes de transport, le village olympique ou les épreuves sur la Seine. Ils ont permis d'identifier des besoins opérationnels complémentaires et communs sur la base desquels les domaines d'expérimentation ont été retenus.

[1] https://www.cnil.fr/fr/deploiement-de-cameras-augmentees-dans-les-espaces-publics-la-cnil-publie-sa-position

Les expérimentations, qui ont reposé à 95 % sur des entreprises et solutions françaises et à 75 % par des PME et *start-up*, ont ainsi porté sur des thèmes très variés :

- commandement, hypervision et collecte et analyse d'informations en source ouverte (OSINT) ;
- cybersécurité et cybercriminalité ;
- exploitation intelligente d'images, agrégation de flux d'images ;
- bulle 3D : contrôle aérien très basse altitude (lutte anti-drone), surveillance aéroportée des sites et abords ;
- NRBC[2] et explosifs ;
- sécurité des espaces nautiques ;
- gestion de flux de personnes et de foules.

Alors qu'elles ont permis une mise en relation inédite entre les forces de sécurité intérieure et les développeurs de solutions innovantes, ces expérimentations ont surtout confirmé la place essentielle du droit dans le déploiement, en France, de technologies de sécurité en appui des forces de sécurité intérieure.

Le défi technologique : un défi avant tout juridique ?

Une contribution qui dépend fortement du contexte juridique et sociétal de chaque pays organisateur

Alors que depuis 20 ans la technologie n'a cessé de prendre une part croissante dans l'organisation des Jeux Olympiques, son possible apport en soutien des dispositifs mis en œuvre pour les sécuriser dépend largement du contexte juridique propre à chaque État organisateur et à l'acceptabilité par sa population des technologies les plus innovantes, comme l'intelligence artificielle.

C'est pourquoi il est apparu nécessaire de définir un cadre légal spécifique au déploiement de nouvelles technologies dans la perspective des JOP 2024.

Le cadre légal des expérimentations

L'intensité des débats au Parlement à l'occasion de l'examen de la loi du 19 mai 2023 relative aux JOP a clairement mis en évidence les enjeux juridiques liés aux développements des nouvelles technologies.

Le recours à deux nouveaux types de technologies est prévu par la loi : d'une part, de façon pérenne, les scanners à ondes millimétriques pour la sécurisation des manifestations culturelles, récréatives ou sportives, d'autre part, à titre expérimental, jusqu'au 31 mars 2025, pour les caméras augmentées.

Dans les deux cas, ce que dit – ou ne dit pas – la loi, est d'ores et déjà riche d'enseignement.

En effet, si les scanners à ondes millimétriques font depuis 15 ans leurs preuves dans les aéroports, les tests grandeur nature conduits depuis l'adoption de la loi, en milieu ouvert, par forte chaleur ou temps de pluie, ont montré que ces technologies n'étaient

[2] Arme nucléaire, radiologique, biologique ou chimique.

aujourd'hui vraisemblablement pas matures pour ce concept d'emploi. Pour autant, si leur utilisation n'avait pas été autorisée par la loi, cette expérimentation, et donc cette prise de conscience, n'aurait pas été possible.

Pour ce qui concerne les caméras augmentées, la loi a retenu un cadre expérimental, ce qui est sans doute plus adapté à la bonne prise en compte des enjeux technologiques et sociétaux.

Ainsi, après avoir clairement posé ce qu'elle interdit, à savoir la reconnaissance faciale et l'interconnexion avec des fichiers, la loi fixe les garanties éthiques auxquelles doit répondre l'expérimentation, en termes de données d'apprentissage, d'enregistrement automatique des signalements pour en assurer la traçabilité, de contrôle humain, de gestion du système pour en corriger les biais éventuels et de possibilité de l'interrompre à tout moment.

Au-delà de ces exigences éthiques « par conception », la loi met également en place un certain nombre de garde-fous : limitation des cas d'usage et des services opérationnels autorisés à recourir à l'expérimentation, sélection des solutions par l'État, autorisation des déploiements par le préfet territorialement compétent, mise en place d'une gouvernance spécifique, évaluation par un comité indépendant, information continue du public, etc.

L'ensemble de ces dispositions, qui peut parfois sembler lourd à mettre en œuvre, offre les garanties d'une démarche incrémentale, nécessaire pour faire évoluer les lignes.

En conclusion

La sécurisation des JOP 2024 est un défi sans précédent, au succès duquel les technologies prendront pleinement leur part.

D'ores et déjà, les premiers enseignements des dispositions autorisées par la loi du 19 mai 2023 pour le déploiement de technologies innovantes, de même que la méthodologie mise en place dans le cadre du programme inédit d'expérimentation conduit par le ministère de l'Intérieur, dessinent des lignes d'action.

Face à la persistance de la délinquance, la diversification des formes de criminalité, notamment organisée, à l'hybridation croissante des menaces dans un contexte de numérisation accélérée et d'explosion de l'intelligence artificielle, les forces de sécurité intérieure et plus largement l'ensemble des acteurs du continuum de sécurité, doivent pouvoir s'appuyer sur des technologies à l'état de l'art, au meilleur coût et lorsque nécessaire souveraines.

Pour y parvenir, il faut pouvoir non seulement fédérer les besoins sur la base de scénarios opérationnels partagés (c'est l'enseignement des expérimentations) mais aussi disposer d'un cadre légal adapté et évolutif, pour ne pas entraver l'innovation tout en préservant systématiquement les libertés fondamentales et individuelles.

La loi du 19 mai 2023 a, à ce titre, sans doute marqué un tournant avec le cadre expérimental des caméras augmentées, mais démontre également, au travers de l'exemple des scanners à ondes millimétriques, comment inscrire dans la loi un choix technologique précis peut introduire des biais non anticipés. Or réviser un cadre législatif prend du temps ; un temps qui n'est pas nécessairement en phase avec des cycles de développement qui ne cessent de se raccourcir.

Le mécano légal et réglementaire nécessaire pour expérimenter des technologies émergentes au profit de la sécurité, sans effet de *stop and go*, reste ainsi partiellement à construire. L'une des pistes pourrait être de sortir d'une logique d'autorisation, technologie par technologie, au profit d'une logique d'expérimentations-cadre par famille d'usage, à conduire dans des lieux préalablement conventionnés où des technologies de

niveaux de maturité variables pourraient être testées sur la base de concepts d'emploi faisant intervenir indifféremment les forces de sécurité intérieure, les polices municipales et les acteurs de sécurité privée.

Cette ambition est l'un des axes de la feuille de route de la direction des entreprises, des partenariats de sécurité et des armes du ministère de l'Intérieur et des Outre-mer, créée à l'été 2023, pour renforcer les partenariats entre les acteurs du continuum de sécurité, en particulier sur le volet industriel et technologique.