Solidaires informatique
Union Syndicale Solidaires

COMMUNIQUE

Jeux olympiques et paralympiques de Paris
Durcissement débridé de la technosurveillance

Les jeux olympiques et paralympiques de Paris fournissent une occasion pour le gouvernement de **durcir l'appareil sécuritaire**. Les effets à anticiper à long terme sont une **surveillance renforcée de la population**, une **augmentation de l'arbitraire policier** et un **affaiblissement des contre-pouvoirs** et recours légaux. La loi spéciale votée pour mettre en œuvre les dernières technologies de surveillance s'inscrit dans des décennies de resserrement de la technosurveillance et offrira des contrats et un terrain de jeu grandeur nature à certaines entreprises du complexe militaro-industriel, tout en leur permettant de soigner leur image. Le tout aux dépends des libertés publiques et de la contestation sociale.

De nouvelles technologies de surveillance légalisées

La loi[1] étend les capacités de surveillance de l'État notamment par l'**introduction de la vidéosurveillance algorithmique** (VSA), un dispositif dont la définition et l'application restent volontairement floues.
La VSA consiste à traiter les images de vidéosurveillance avec des programmes automatisés (algorithmes). Ces programmes visent généralement à y reconnaitre des *« comportements suspects »* afin de **réprimer préemptivement** d'éventuels *« troubles »*.
Les dispositifs mis en place sont censés prendre **fin le 31 mars 2025**, bien après la fin des jeux. Cette loi s'inscrit donc dans une longue batterie d'essais sécuritaires.

Comment la VSA est légalisée

Les images de vidéosurveillance pourront faire l'objet de *« traitements algorithmiques »*, afin de *« détecter, en temps réel, des événements prédéterminés susceptibles de présenter ou de révéler ces risques »*. La nature de ces traitements est laissée floue et sera précisée par décret, c'est-à-dire **à la discrétion du gouvernement**.
Ces traitements concerneront désormais aussi les **vidéos prises depuis les drones** (*« aéronefs »* dans la loi) et **les caméras des équipes SNCF et RATP**. La loi élargit aussi le périmètre de la surveillance auquel ces équipes ont accès : elles peuvent maintenant faire appel à la vidéosurveillance des **abords immédiats des gares**, et pas seulement des images *« relevant respectivement de leur compétence »*.
Une part des images collectées pourra être utilisée comme ***« données d'apprentissage »* pour affiner les traitements algorithmiques**. Elles seront détruites 12 mois après. Ceci laisse entendre que le législateur entend donner suite à la VSA en la perfectionnant et **l'installant durablement dans le paysage sécuritaire français**.

Pour résumer, on a : mise en place de police prédictive via le traitement d'images ; élargissement des sources de captation vidéo ; utilisation des images pour pérenniser le système sur le long terme.

contact@solidairesinformatique.org
@solidairesinformatique
@SolinfoNat
@solidairesinformatique
@SolInfoNat@syndicat.solidaires.org
www.solidairesinformatique.org

COMMUNIQUE

Contre-pouvoirs et recours légaux réduits

C'est la Commission nationale de l'informatique et des libertés (CNIL) qui est censée veiller au respect de la vie privée lorsque des données personnelles sont traitées par des systèmes informatisés.

La nouvelle loi écarte la CNIL en réduisant son pouvoir de contrôle, notamment au profit de la seule *« commission départementale de vidéoprotection »*. Par exemple, la CNIL ne pourra plus ordonner au préfet la suspension d'un système de vidéosurveillance. La loi retire aussi au gouvernement l'obligation de faire un rapport d'activité de la videosurveillance à la CNIL, ce qui entérine une situation de fait : le dernier rapport date de 2014.

La loi allège les peines pour les personnes qui entraveraient les contrôles de la commission départementale de vidéoprotection : jusqu'ici passible de 3 ans de prisons et 45 000€ d'amende, le délit d'entrave n'est plus passible que de 1 an de prison et 15 000€ d'amende.

La possibilité pour une personne d'avoir accès aux enregistrements vidéo la concernant est réduite. Le droit de recours à la CNIL est supprimé, ainsi que la mention de *« l'accès de droit »*.

L'esprit de la loi semble donc être : davantage de vidéosurveillance, quel qu'en soit le prix à payer sur les libertés publiques.

Surveillance individuelle et répression par d'autres moyens

Outre la VSA, **la loi facilite les consultations de casier judiciaire** de toutes les personnes ayant accès aux établissements sportifs listés dans le futur décret. Elle alourdit les peines pour les personnes s'introduisant frauduleusement dans ces établissements.

Les *« dispositifs d'imagerie à ondes millimétrique »*, c'est-à-dire des **scanners corporels permettant de voir à travers les vêtements** d'éventuels objets dissimulés, sont mentionnés. Il s'agit une fois encore d'expérimenter et étendre l'usage d'une technologie intrusive, qui est actuellement limitée à quelques aéroports.

Évènements sportifs : un prétexte au durcissement sécuritaire depuis longtemps

Le contrôle numérique des spectatrices et spectateurs n'est pas nouveau. En France, les personnes interdites de stade sont fichées et la répression associée est durcie régulièrement.

Dans le monde, l'organisation de jeux olympiques et paralympiques est **systématiquement accompagnée d'un durcissement technosécuritaire**. Pour prouver que la ville-hôte peut accueillir massivement des touristes tout en anticipant tous les risques, la proportionnalité vis-à-vis des atteintes aux libertés publiques est sacrifiée.

C'est pourquoi on constate **la mise en place dans l'espace public de matériel de guerre et de tactiques initialement à buts contre-insurrectionnel et colonialiste tels les contrôles biométriques et la surveillance par drone.** Des entreprises du complexe militaro-industriel peuvent tester leurs nouvelles technologies à grande échelle tout en soignant leur image de marque. L'expérience montre que les mesures d'exceptions adoptées pour sécuriser les jeux sont pérennisées.

Ces investissements, déploiements massifs et mesures liberticides pérennisées sont à mettre en perspective avec le fait que les jeux durent moins de 3 semaines et sont un spectacle offert par une poignée d'athlètes pour quelques milliers de spectatrices et spectateurs privilégié·es.

COMMUNIQUE

Football en France : répression de la contestation politique dans les stades

La surveillance des spectatrices et spectateurs a commencé en 2007 avec la création du Fichier national des interdits de stade (FNIS)[2], l'objectif affiché étant la prévention des violences. L'interdiction de stade est prononcée par un juge administratif ou judiciaire et une personne inscrite au fichier y reste 5 ans de plus après l'expiration de la mesure à son encontre.

En 2013, le Paris-Saint-Germain a mis en place, conjointement avec la police, un **fichage arbitraire de supporteurs et supportrices considéré·es comme indésirables**. Ce fichier a été jugé illégal par la CNIL… Pour être rendu légal en 2016. Il autorise la police à ficher toute personne qu'elle estime être supporteur·trice et l'autorise à communiquer ces données aux clubs, qui sont des entités privées[3].

Cela permet aux clubs de faire taire des personnes et groupes qui, par exemple, critiqueraient la politique d'un club et risqueraient de nuire aux bénéfices de ses actionnaires. Contester publiquement (avec une banderole, par exemple) contre une politique de prix excluant les classes populaires est notamment devenu plus difficile.

Jeux olympiques et paralympiques : un historique de militarisation de l'espace public

Un petit historique nous renseigne sur la consistance avec laquelle **les jeux donnent l'occasion de tester et pérenniser des technologies de surveillance issues du domaine militaire**, dans le but de pacifier l'espace public et/ou de favoriser des intérêts privés.

À Athènes en 2004, les caméras de surveillance et leur système informatique associé installés pour les jeux sont restés après les évènements. La police a, plus tard, tenté de l'utiliser pour contrôler les soulèvements contre l'austérité.

En 2012 à Londres, une loi spéciale a permis la mise en place de cartes d'identification biométriques, de systèmes de reconnaissance de plaques d'immatriculation et de reconnaissance faciale. Militairement, c'était la plus grosse opération sur le sol britannique depuis 1945. Partager la connexion 3G de son téléphone a été interdit afin de préserver le monopole des points d'accès payants wifi de l'opérateur BT, et une milice spécifique a été créée pour faire la chasse à ces points d'accès. La loi interdisait aussi la publication sur internet de vidéos prises dans l'enceinte des jeux, pour préserver les droits exclusifs des chaines et la propriété intellectuelle du Comité international olympique (CIO).[4]

À Sotchi en 2014, c'est le service de renseignement intérieur russe (FSB) qui a été directement chargé de préparer la sécurité des jeux. Il a utilisé l'occasion pour améliorer le système d'interception de masse des télécommunications Sorm[5] et veillé à son installation chez les opérateurs de la région. La 4G a été installée à Sotchi mais cela a surtout été l'occasion d'installer des technologies massives et intrusives de collecte et d'analyse du trafic internet. Des drones et caméras ont été mis en place, le tout associé à diverses interdictions, comme celle de manifester. La surveillance de masse du trafic internet de cette région se poursuit après les jeux.[6]

En 2022 à Pékin, les jeux arrivaient dans un pays aux libertés publiques déjà fortement restreintes, d'autant plus avec la pandémie de covid. Une des nouveautés a été l'application pour smartphone « MY2022 » diffusée par le gouvernement chinois. Destinée officiellement à prévenir la pandémie, elle collectait nombre de données personnelles et de santé à destination des autorités chinoises. Elle était aussi truffée de failles de sécurité et comportait une liste de mots potentiellement interdits pour les gens l'utilisant pour communiquer.[7]

COMMUNIQUE

Les villes françaises comme laboratoires

L'exploitation informatisée des images vidéo est établie depuis plusieurs années en France, malgré son illégalité dans la plupart des cas. Les caméras étant désormais répandues, des entreprises vendent aux villes des logiciels d'analyse des images, comme *Briefcam* dont le logiciel est utilisé dans au moins 35 villes de France et permet de faire de la reconnaissance faciale et de trier les vidéos selon les attributs physiques d'une personne. Dans le même genre, *Map Revelation*, qui se félicite de pouvoir prédire crimes et délits, analyse entre autres Montauban et Montpellier.

À Paris, la gare de Châtelet les Halles est présentée comme un laboratoire de la RATP pour tester des méthodes de surveillance, avec l'entreprise Axone. **Certaines caméras captent même le son**, par exemple lors du test du dispositif DéGIV (Détection et Gestion d'Incident en Véhicule ferroviaire) sur la ligne 14.

Montées sur drones, les caméras deviennent mobiles. C'était le cas à Paris et Istres lors des manifestations retraites. Pendant le confinement, l'entreprise Drones06 a équipé Cannes avec des drones à caméra et haut-parleur pour rappeler à l'ordre les passant·es et permettre l'envoi éventuel d'agent·es.

Au-delà de la surveillance, ce sont aussi **des cas flagrants de privatisation de la sécurité publique**, les vidéos et leur analyse étant confiées à des entreprises. À Suresnes par exemple, les images sont mises à disposition de l'entreprise XXII, qui est contractuellement propriétaire des données. Lors du test, l'entreprise a même pu inviter d'autres clients au centre de surveillance urbain de la ville.[8]

Le site Technopolice cartographie les différentes méthodes de surveillance utilisées.[9]

COMMUNIQUE

Comprendre et anticiper les effets de la VSA

L'expérience des mesures liberticides d'exception nous indique que ce qui est mis en place pour les jeux de Paris aura sans doute **vocation à être pérennisé**, la trouille sécuritaire du pouvoir et l'appât du gain du capitalisme de surveillance étant puissants.

La suite de la fuite en avant

Cette nouvelle étape dans l'évolution de la vidéosurveillance continue la fuite en avant commencée avec la généralisation des caméras. Face au manque de résultats sur les chiffres de la délinquance, les industriels ont d'abord enjoint les décideur·euses à installer plus de caméras, sans plus de résultat. Il fallut alors plus de personnels afin de surveiller les écrans derrière ces caméras. À nouveau, **aucune étude n'a pu corréler une baisse de la délinquance** à cette surenchère.

La nouvelle solution miracle vantée par les professionnel·les du secteur serait encore un nouvel investissement d'argent public dans une assistance algorithmique supposée enfin justifier des années de gâchis, et ce toujours **sans étude permettant de justifier ce choix**. Et si ces installations et procédés n'ont pas d'impact sur la délinquance, ils ont en revanche de véritables impacts sur les libertés publiques.[10]

Une police prédictive basée sur des algorithmes discriminatoires, opaques et mal compris

La VSA est fondée sur l'idée de **déterminer automatiquement si un comportement filmé est *« normal » ou « anormal »***, pour déclencher une alerte au besoin. Le but est de remplacer ou compléter le visionnage manuel effecuté par les agent·es des centres de surveillance urbains (CSU).

La VSA utilise des algorithmes d'apprentissage automatique (machine learning), qui connaissent ces dernières années un boom d'applications diverses. Pour lui faire *« apprendre »*, on nourrit l'agorithme avec des exemples de situations en lui indiquant pour chacune si elle est *« normale »* ou non.

L'algorithme est ensuite censé déterminer seul si une nouvelle situation mérite le déclenchement d'une alerte. Cette alerte permet de déclencher une intervention sur une situation suspecte avant qu'un délit ne soit commis : **c'est de la police prédictive.**

Premier problème : l'apprentissage, qui est donc un élément central pour identifier correctement les situations, est **confié à la police et aux entreprises privées dans une complète opacité**.

Second problème : aujourd'hui, même la recherche scientifique n'est pas tout le temps capable d'expliquer quels critères ont été utilisés par un algorithme pour établir ses choix. Pour la VSA, cela signifie qu'**on ne saura parfois pas comment la décision de lever une alerte est prise**, rendant impossible l'établissement de responsabilité.

En fin de compte, cette surveillance risque de **suspecter toute personne utilisant la rue pour autre chose que circuler d'un point A à un point B** et va accroitre la stygmatisation des plus précaires, comme les personnes vivant dans la rue. Il s'agit d'une normalisation de l'espace public sans garde-fou, dont l'opacité empêche tout contrôle efficace, dont l'utilisé pour la sécurité n'est pas prouvée, mais qui sert des intérêts économiques et sécuritaires.[11] Sa mise en place amorce la légalisation de la surveillance biométrique.

COMMUNIQUE

La surveillance biométrique comme prochaine étape

La surveillance biométrique est déjà à l'œuvre ailleurs, avec par exemple le système de reconnaissance faciale Red Wolf en Israël. Dans ce contexte de répression militarisée, il permet aux autorités israéliennes de scanner le visage des Palestien·nes à leur insu aux points de contrôle. Relié à des bases de données, **il permet en un instant de récupérer les informations connues concernant la personne et ses relations**. Ce contrôle est complété par des milliers de caméras de surveillance déployées dans les zones urbaines. Ensemble, caméras et reconnaissance faciale ont un effet dissuasif sur les personnes qui souhaiteraient manifester dans l'espace public.
Amnesty International a contacté les entreprises fournissant ces caméras[12], et elles n'ont pas su expliquer comment elles s'acquittaient de leur responsabilité en matière de droits humains, en contradicttion avec les principes directeurs de l'ONU.[13]

Pour résumer...

- Les jeux de Paris sont un **prétexte à la légalisation et mise en place à long terme de la VSA et à la réduction des contre-pouvoirs régulant la surveillance et le fichage**
- Cette mise en place prolonge des **années d'accroissement de la surveillance de l'espace public et de développement technologique sécuritaire** testé dans les villes et dans les rencontres sportives en France et ailleurs, **sans que leur efficacité soit prouvée**
- L'opacité de la création des algorithmes par des entreprises et de leur exploitation par la police, associée à la réduction des contre-pouvoirs et recours légaux, **augmentera l'arbitraire policier, facilitera les dérives, opprimera l'expression populaire et brouillera l'établissement de responsabilités**
- Les mécanismes d'apprentissage des algorithmes **renforceront les biais discriminatoires** et stygmatisants
- Ce processus contribue à **militariser l'espace public** et ouvre la voie au resserrement de la surveillance avec la reconnaissance faciale
- De nombreuses entreprises liées au secteur militaro-industriel et au capitalisme de surveillance vont bénéficier de cette évolution et vont **continuer à encourager cette fuite en avant technosécuritaire**

[1] https://www.vie-publique.fr/loi/287639-jo-2024-loi-du-19-mai-2023-jeux-olympiques-et-paralympiques
[2] https://fr.wikipedia.org/wiki/Interdiction_de_stade
[3] http://www.regards.fr/archives/web/article/les-supporters-de-football-cobayes-du-fichage-et-de-la-surveillance-generalisee
[4] https://www.theguardian.com/sport/2012/mar/12/london-olympics-security-lockdown-london (en anglais)
[5] https://fr.wikipedia.org/wiki/SORM
[6] https://www.theguardian.com/world/2013/oct/06/sochi-olympic-venues-kremlin-surveillance (en anglais)
[7] https://www.liberation.fr/international/asie-pacifique/my2022-lappli-officielle-des-jo-de-pekin-est-elle-un-espion-planque-dans-la-poche-des-participants-20220203_ZPQUTSHHQZCOTI5T4QEKXWPCJI/
[8] https://technopolice.fr/blog/les-suresnois%C2%B7es-nouveaux-cobayes-de-la-technopolice/
[9] https://technopolice.fr
[10] https://www.laquadrature.net/2023/01/18/non-a-la-videosurveillance-algorithmique-refusons-larticle-7-de-la-loi-olympique/
[11] https://www.laquadrature.net/biometrie-jo/
[12] https://www.amnesty.fr/actualites/comment-israel-renforce-son-controle-sur-les-palestiniens-via-la-reconnaissance-faciale
[13] https://www.ohchr.org/fr/publications/reference-publications/guiding-principles-business-and-human-rights-implementing