NON AU PROJET DE LOI SUR LA VIDEOSURVEILLANCE ALGORITHMIQUE

OUI A UN DEBAT CITOYEN SUR L'INTELLIGENCE ARTIFICIELLE

Le 31 janvier 2023, le Sénat a adopté en première lecture, le projet de loi relatif aux Jeux Olympiques et Paralympiques de 2024.

Le projet de loi comprend plusieurs mesures, concernant divers domaines, nécessaires à l'organisation des jeux. Ces mesures font l'objet de vingt articles répartis en cinq chapitres, respectivement intitulés « Adaptations nécessaires en matière d'offre de soins et de formation aux premiers secours », « Mesures visant à renforcer la lutte contre le dopage », « Dispositions visant à mieux garantir la sécurité », « Dispositions diverses », « Dispositions relatives à l'outre-mer ».

Usage de la vidéoprotection intelligente, scanners corporels à l'entrée des stades, ouverture des magasins le dimanche… Le projet de loi prévoit plusieurs dérogations ou expérimentations pour assurer le bon déroulement des Jeux olympiques de 2024 en matière de sécurité, de soins, de lutte antidopage ou de transports.

Nombre de ces mesures ont un caractère permanent et sont conçues pour s'appliquer y compris en dehors de la période des jeux Olympiques et Paralympiques. Ainsi, si huit articles ne sont applicables qu'aux prochains jeux Olympiques et Paralympiques de 2024, dont deux ont un caractère expérimental, onze autres articles créent des dispositions nouvelles ou modifient des dispositions existantes de façon pérenne et seront donc susceptibles de s'appliquer à d'autres situations.

Le Gouvernement se propose d'expérimenter, pour une période prenant fin le 30 juin 2025, la possibilité de recourir à des traitements de données comportant des systèmes d'intelligence artificielle appliqués aux images de vidéoprotection, pour mieux assurer la sécurité d'évènements sportifs, festifs ou culturels, particulièrement exposés à des risques, notamment de nature terroriste.

« Le recours, jusqu'ici inédit en France, à un tel traitement aux fins d'exercice des missions de maintien de l'ordre et de prévention des atteintes à la sécurité des personnes et des biens, s'il est limité, dans le projet de loi, à la protection de certains événements, est néanmoins susceptible de mettre en cause la protection de la vie privée et d'autres droits et libertés fondamentales, tels que la liberté d'aller et venir et les libertés d'opinion et de manifestation, lorsque ces dernières s'exercent à l'occasion de ces événements. (Avis du Conseil d'Etat n° 406383) »

L'article 7 du projet de loi, qui prévoit la mise en place provisoire de la vidéosurveillance dite intelligente, constitue une menace réelle pour les droits et libertés dès lors qu'il autorise une *« phase d'expérimentation »* dans l'espace public sans aucune garantie quant à son démantèlement une fois les JO terminés. Les cameras seront installées, payées par le contribuable et opérationnelles, elles ne seront pas démontées.

La prolifération dans l'espace public, parfois même de façon occulte, de dispositifs de cameras dites « *augmentées* » ou « *intelligentes* »,ou VSA (Video Surveillance Algorithmique) improprement dénommés dispositif de video protection, pose de nouvelles questions sur les enjeux de ces dispositifs au regard des libertés individuelles des personnes dont l'image est enregistrée en dehors de tout cadre juridique approprié, et au mépris des dispositions du RGPD (Règlement Général sur la Protection des Données).

La notion de caméra ou vidéo « augmentée » désigne des dispositifs vidéo auxquels sont associés des logiciels permettant une analyse automatique de l'image afin de détecter par exemple des formes ou des objets, d'analyser des mouvements, etc. Cette intelligence artificielle envoie une alerte à la police dès qu'elle détecte un comportement ou une situation qu'elle a été entraînée à reconnaitre et à identifier comme anormale. C'est l'État et les collectivités territoriales — ou les entreprises privées qui fournissent ces logiciels — qui déterminent les comportements et définissent les alertes susceptibles de notifications.

Ces caméras sont, par nature, très différentes de celles traditionnellement déployées : les personnes ne sont plus seulement filmées mais analysées de manière automatisée, en temps réel, afin de collecter certaines informations les concernant.

Ces nouveaux outils vidéo peuvent conduire à un **traitement massif de données personnelles**, potentiellement à l'insu des personnes du fait du caractère « *invisible* » des logiciels d'analyse d'images associés aux caméras.

Et ce, alors que cette technologie n'a jamais fait preuve de son efficacité. *« Aucune étude ou évaluation sérieuse ne montre qu'elle est efficace pour lutter contre la criminalité »*, précise à *Reporterre* Katia Roux, responsable plaidoyer Technologies et droits humains à Amnesty International France.

Le rapport de la Cour des comptes de 2020 rappelle qu'« *aucune corrélation globale n'a été relevée entre l'existence de dispositifs de vidéoprotection et le niveau de la délinquance commise sur la voie publique, ou encore les taux d'élucidation* ». Quant au laboratoire de recherche de la CNIL, le LINC, il affirme après avoir passé en revue l'état de l'art que « *la littérature académique, en France et à l'international […], a démontré que la vidéosurveillance n'a pas d'impact significatif sur la délinquance* ».

L'évaluation publique des dispositifs actuels n'ont permis de démontrer la moindre baisse du taux de délinquance ni la moindre une incidence sur le taux d'élucidation des délits après leur installation, pas plus que n'a été identifié leur réel besoin ou intérêt scientifique alors même que les études indépendantes menées sur le sujet pointent toutes vers le caractère dérisoire du rapport cout/bénéfice de cet outil.

Le gouvernement justifie pourtant la mise en place de ce dispositif par la nécessité d'*« assurer la sécurité de manifestations sportives, récréatives ou culturelles qui, par leur ampleur ou leurs circonstances, sont particulièrement exposées à des risques d'actes de terrorisme ou d'atteinte grave à la sécurité des personnes »*. Treize millions de spectateurs sont attendus lors des Jeux olympiques de Paris.

Le risque d'une surveillance généralisée induit par la multiplication des dispositifs vidéo, pointé depuis longtemps par la CNIL, prend aujourd'hui une nouvelle dimension avec l'essor des dispositifs de vidéo *« augmentée »* : **cette surveillance se double d'une analyse des personnes**.

Le déploiement de ces dispositifs dans les espaces publics, où s'exercent de nombreuses libertés individuelles (liberté d'aller et venir, d'expression, de réunion, droit de manifester, liberté de culte, etc.), présente incontestablement des risques pour les droits et libertés fondamentaux des personnes et la préservation de leur anonymat dans l'espace public.

Ces dispositifs posent également de nouveaux enjeux pour les personnes lorsqu'ils ont vocation à **automatiser entièrement certaines activités de la vie courante**. Des actes simples de la vie quotidienne pourraient ainsi être filmés et analysés par des caméras « augmentées », renforçant encore le sentiment de surveillance des personnes à mesure que ces dispositifs se généraliseront dans les espaces publics : rues, transports, commerces, lieux culturels et sportifs, etc.

Ce projet constitue un l'état un risque majeur pour les libertés individuelles et il convient d'en être particulièrement conscient.

« ***Les technologies d'intelligence artificielle peuvent avoir des effets négatifs, voire catastrophiques si elles sont utilisées sans prendre suffisamment en compte la manière dont elles affectent les droits humains*** », a déclaré Michelle Bachelet, la Haut-Commissaire des droits de l'homme de l'ONU.

Face à la capacité de l'IA à alimenter des violations des droits de l'homme à « *une échelle colossale* », les services de Mme Bachelet appellent la planète à agir dès maintenant. **« *Plus les risques pour les droits de l'homme sont élevés, plus les obligations légales relatives à l'utilisation des technologies de l'IA devraient être strictes* »**, a affirmé la Haut-Commissaire.

La France ne doit pas devenir un pays comme la Chine, où la préservation de la vie privée a disparu dans l'espace public et disparait progressivement dans la sphère privée.

N'oublions jamais le pacte fondateur de la République : **LIBERTE- EGALITE- FRATERNITE**. C'est le seul ciment du pacte social et du vivre ensemble dans la République.

Il faut s'en rappeler chaque jour, c'est lui qui donne du sens à l'action citoyenne !

Ces outils de surveillance biométrique sont **intrinsèquement dangereux** et ne peuvent être contenus par **aucun garde-fou**, qu'il soit légal ou technique. Les accepter c'est faire sauter les derniers remparts qui nous préservent d'une société de surveillance totale.

A l'heure ou le Haut-Commissariat aux droits de l'homme (HCDH) a appelé la communauté internationale à imposer un moratoire sur certains systèmes d'intelligence artificielle, comme la reconnaissance faciale, le temps de mettre en place un dispositif pour protéger les droits humains quant à leur utilisation, ce projet de loi constitue un risque majeur pour les libertés individuelles et une atteinte sans précédent à la protection de la vie privée dans l'espace public.

LE RECOURS A L'INTELLIGENCE ARTIFICIELLE NECESSITE UN DEBAT CITOYEN A LUI SEUL CAR C'EST UN CHOIX DE SOCIETE : IL NE PEUT ETRE RAISONNABLEMENT DEBATTU EN URGENCE AU PARLEMENT A L'OCCASION D'UNE LOI SUR LES JEUX OLYMPIQUES AU REGARD DES INCIDENCES CATASTROPHIQUES POUR LES DROITS HUMAINS DONT IL EST POTENTIELLEMENT PORTEUR

ARGUMENTAIRE : LA QUADRATURE DU NET

https://www.laquadrature.net/biometrie-jo/

La VSA est par essence un outil de surveillance totale

La VSA n'est pas un simple logiciel : elle analyse **des milliers d'heures de vidéos pour catégoriser les comportements** suivant ce que les autorités auront qualifié de « suspect » ou « anormal » pour l'appliquer en temps réel sur les caméras de surveillance. **Cela crée un gigantesque système de ciblage « d'anomalies »** afin d'automatiser le travail de la police. Il s'agit d'un réel changement de dimension de la surveillance et d'industrialisation du travail d'image pour **démultiplier les notifications et interpellations**, guidées par cette intelligence artificielle.

La VSA existe déjà et elle est déployée dans l'opacité

Déployée ces dernières années en toute opacité, la VSA est une technologie quasiment inconnue de la population. **Développée et vendue discrètement par des entreprises**, elle est implantée sans information par les collectivités, empêchant les habitant·es d'avoir facilement accès à ce qui est installé dans leur ville. Ce déploiement ne répond pas à un besoin démocratique mais **à des logiques économiques** alors qu'aucune preuve d'efficacité n'existe.
Par exemple, le logiciel de l'entreprise Briefcam, déployé en catimini dans plus de 200 municipalités en France, permet de réaliser **des recherches par attributs** (couleur des vêtements, couvre-chef, sac, type de vêtement et supposé genre de la personne), de faire du **suivi de personne** à travers toutes les caméras de la ville et possède même **l'option « comparaison faciale »** qui permet de faire une recherche parmi les flux vidéos du visage identifié. C'est grâce à un long travail de documentation de notre part et d'investigation de journalistes qu'il a été possible de comprendre ce que peut réellement faire ce fameux logiciel de VSA le plus vendu en France.
Cette opacité rend totalement impossible l'expression d'un choix démocratique sur la question.

La VSA n'est pas moins dangereuse que la reconnaissance faciale

La VSA et la reconnaissance faciale reposent sur les mêmes algorithmes d'analyse d'images et de surveillance biométrique. La seule différence est que la première isole et reconnaît des **corps**, des mouvements ou des objets, lorsque la seconde détecte un **visage**. Ce sont généralement les **mêmes entreprises** qui développent ces deux technologies. Par exemple, la start-up française Two-I s'est d'abord lancé dans la détection d'émotion, a voulu la tester dans les tramways niçois, avant d'expérimenter la reconnaissance faciale sur des supporters de football à Metz. Finalement, l'entreprise semble se concentrer sur la VSA et en vendre à plusieurs communes de France. **La VSA est une technologie biométrique intrinsèquement dangereuse, l'accepter c'est ouvrir la voie aux pires outils de surveillance.**

La France est la cheffe de file de l'Europe en terme de surveillance

Avec cette loi, la France sera le premier État membre de l'Union européenne à légaliser et autoriser la surveillance biométrique, à l'opposée d'autres positions au sein de l'UE. Les discussions en cours sur le règlement européen sur l'intelligence artificielle envisagent même son interdiction formelle. **La France confirmerait sa place de cheffe de file de la surveillance en Europe**, s'éloignant toujours plus des idéaux de respect des droits fondamentaux et se rapprochant de la culture de la surveillance d'autres pays plus autoritaires. Les pays qui ont profité d'évènements sportifs pour tester et rendre acceptables des technologies de surveillance sont la Russie, la Chine et le Qatar.

Aucun garde-fou possible pour la VSA

Pour faire des traitements d'images pointus et reconnaître des formes avec précision, les algorithmes de VSA doivent être basés sur une technologie complexe dite de « deep learning » qui fonctionne grâce à des calculs si sophistiqués qu'ils dépassent l'entendement humain. L'algorithme décide lui-même quels paramètres sont pertinents pour détecter un évènement, sans qu'il soit possible de savoir lesquels ont été retenus pour donner le résultat. **Il est impossible de garantir que le logiciel n'exploitera pas de données sensibles** et de caractéristiques biométriques. Même **les concepteurs de ces algorithmes n'ont pas de visibilité sur les données qu'ils exploitent**. Ces technologies sont intrinsèquement dangereuses et ne pourront jamais être limitées efficacement sur le plan légal ou technique. **Le seul garde-fou envisageable est l'interdiction de leur usage sur des activités humaines filmées dans l'espace public**.

Réponses aux contre-arguments

« La VSA sera expérimentée uniquement pour les Jeux Olympiques »

Faux, les Jeux olympiques ne sont pas une expérimentation : la VSA est déjà déployée en toute opacité et illégalité et continuera à l'être après. On a retrouvé des traces de contrat entre la ville de Toulouse et IBM pour détecter des comportements anormaux dès 2017, on compte au bas mot **deux cent villes en France qui l'emploient** et elle s'installe aussi dans les magasins. Il y a donc un projet politique de long terme et les JO ne sont qu'un prétexte pour tenter de légaliser cette technologie.

Après les Jeux, **la vidéosurveillance algorithmique sera généralisée** : une fois que des dizaines de milliers d'agents de sécurité et de police seront formés, que la technologie sera achetée et mise au point grâce à des fonds publics, il faudra bien la rentabiliser. Son abandon après cette soi-disant expérimentation est donc illusoire.

« La VSA est seulement une aide à la décision »

Faux, la VSA n'est pas une simple aide technique : pour la concevoir, **les entreprises doivent prendre une série de décisions morales et subjectives** (qu'est-ce qu'un comportement « suspect » ?). Son application est également politique puisque la **VSA est un instrument de pouvoir donné à des services coercitifs**. La VSA n'est pas un outil neutre mais analyse en permanence les corps et les déplacements, en particulier de celles et ceux qui passent le plus de temps dans la rue. Se cacher derrière une machine, c'est déresponsabiliser les choix des agents de sécurité : « c'est pas nous qui avons ciblé cette personne, c'est l'algorithme ». C'est aussi accepter la **déshumanisation du rapport des citoyens avec l'État**, qui finira par ne prendre que des décisions automatisées sur sa population comme cela commence à être le cas avec la vidéoverbalisation. La VSA n'est pas une « aide à la décision » mais constitue bien un changement d'échelle dans les capacités de surveillance de l'État.